Designing and Deploying 802.11n Wireless Networks

Gain a practical understanding of the underlying concepts of the 802.11n standard and the methodologies for completing a successful wireless network installation

ciscopress.com

Jim Geier

Designing and Deploying 802.11n Wireless Networks

Jim Geier

Copyright © 2010 Cisco Systems, Inc.

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America

First Printing June 2010

Library of Congress Cataloging-in-Publication Data

Geier, James T.
Designing and deploying 802.11n wireless networks / Jim Geier.
p. cm.
ISBN 978-1-58705-889-9 (hardcover)
1. Wireless LANs. 2. IEEE 802.11 (Standard) I. Title.

TK5105.78.G448 2010
004.6'8--dc22

2010019130

ISBN-13: 978-1-58705-889-9

ISBN-10: 1-58705-889-8

Warning and Disclaimer

This book is designed to provide information about wireless networking, which includes Cisco products. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States please contact: **International Sales** international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Executive Editor: Mary Beth Ray

Managing Editor: Sandra Schroeder

Senior Development Editor: Christopher Cleveland

Project Editor: Mandie Frank

Editorial Assistant: Vanessa Evans

Cover and Interior Designer: Louisa Adair

Composition: Mark Shirar

Cisco Representative: Erik Ullanderson

Cisco Press Program Manager: Anand Sundaram

Technical Editors: Tom Carpenter and Christian Estes

Copy Editor: Keith Cline

Indexer: Bill Meyers

Proofreader: Kathy Ruiz

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Introduction

The 802.11n amendment to the IEEE 802.11 wireless LAN (WLAN) standard was ratified in September 2009, and enables 802.11 systems to provide much higher performance and range than before. The majority of network equipment manufacturers now offer 802.11n-compliant equipment as their primary WLAN solution. WLANs based on earlier versions of the standard (802.11a, 802.11b, and 802.11g) are considered "legacy," and there is significant risk that these existing non-802.11n systems will become obsolete. As a result, organizations deploying new WLANs should definitely implement 802.11n-compliant equipment. In addition, organizations with existing non-802.11n WLANs should begin planning the migration to 802.11n-compliant networks.

This how-to book focuses on planning, designing, installing, testing, and supporting 802.11n wireless networks for a variety of applications. The methods, recommendations, and tips in this book are based on the author's many years of practical experience deploying WLANs. Organizations with no existing wireless network and those migrating from legacy wireless networks to 802.11n-compliant networks will find this book to be a valuable guide.

Goals and Methods

The overall goal of this book is to guide you through the steps of deploying an 802.l1n WLAN. To accomplish this, the book includes the following elements:

- **Step-by-step approaches:** The book breaks each phase of WLAN deployment into clearly defined steps that provide the basis for understanding and planning the details of the phase.
- **Case studies:** The book includes several case studies that provide explanations of concepts and methods as they are practiced in actual deployments.
- **Hands-on exercises:** The book includes exercises that make use of free and inexpensive tools that help you gain practical experience with concepts described in the chapter.
- **Tips:** Concise tips are distributed throughout the book and provide insightful information related to deploying WLANs.

Who Should Read This Book?

This book is intended for a variety of people, from someone with basic knowledge of networking to others who might have years of experience working with WLANs but have little if any experience implementing 802.11n networks.

How This Book Is Organized

Although this book can be read cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to learn just the information that you need.

This book covers the following topics:

- Part I, "Fundamental Concepts": This part of the book includes chapters that cover important underlying concepts that must be understood before deploying an 802.11n wireless network. Readers already familiar with WLANs may be able to skip one or more of the chapters in this part of the book.
  - Chapter 1, "Introduction to Wireless Networks": This chapter defines the markets and applications of WLANs and the wireless technologies that support them.
  - Chapter 2, "Radio Wave Fundamentals": This chapter explains radio wave fundamentals so that you have the basis for understanding the complexities of deploying WLANs.
  - Chapter 3, "Wireless LAN Types and Components": This chapter describes ad hoc, mesh, and infrastructure WLAN types and various components, such as access points, controllers, client radios, amplifiers, and others.
  - Chapter 4, "Wireless LAN Implications": This chapter explains the impacts of radio signal interference, security vulnerabilities, multipath propagation, roaming, and battery limitations on WLANs.
- Part II, "The 802.11 Standard": This part of the book includes chapters that contain in-depth coverage of the most current medium access and physical layers of the IEEE 802.11 standard (including 802.11n functionality). The focus here is on the elements of the standard that readers should know to be successful at deploying and supporting 802.11n wireless networks.
  - Chapter 5, "Introduction to IEEE 802.11 and Related Standards": This chapter provides a background and importance of 802.11 standards and an overview of the 802.11 standard and related standards, such as IEEE 802.2.
  - Chapter 6, "IEEE 802.11 Media Access Control (MAC) Layer": This chapter explains details of the 802.11 standard that you need to know to help you best configure and troubleshoot 802.11n WLANs.
  - Chapter 7, "IEEE 802.11 Physical (PHY) Layers": This chapter describes the modulation functions that are part of the 802.11n physical layer and legacy physical layers (802.11a, 802.11b, and 802.11g).

- Part III, "Wireless Network Design": This part of the book includes chapters that cover steps necessary to design an 802.11n wireless network for various scenarios.
  - Chapter 8, "Planning a Wireless LAN Deployment": This chapter provides an overview of the steps that you should complete when deploying a WLAN and details on defining the project scope, developing a work breakdown structure, identifying staffing, creating a schedule, developing a budget, evaluating risks, and analyzing feasibility.
  - Chapter 9, "Defining Requirements for a Wireless LAN": This chapter explains how to gather, analyze, and document requirements for an 802.11n WLAN.
  - Chapter 10, "System Architecture Considerations": This chapter explains what to consider when designing the access network and distribution system for an 802.11n WLAN.
  - Chapter 11, "Range, Performance, and Roaming Considerations": This chapter explains the various tradeoffs for enhancing the range, performance, and roaming capabilities of an 802.11n wireless LAN.
  - Chapter 12, "Radio Frequency Considerations": This chapter covers important radio frequency (RF) design considerations for 802.11n WLANs, such as frequency band selection, transmission channel settings, difficult-to-cover areas, and radio signal interference reduction techniques.
  - Chapter 13, "Security Considerations": This chapter explains important methods and techniques for securing a WLAN, including encryption, authentication, rogue access point detection, RF shielding, and security polices.
- Part IV, "Wireless Network Installation and Testing": This part of the book includes chapters that explain the steps necessary to install and test an 802.11n wireless network.
  - Chapter 14, "Test Tools": This chapter describes the tools that you need to effectively design and support an 802.11n WLAN.
  - Chapter 15, "Performing a Wireless Site Survey": This chapter explains the steps and techniques, such as inspecting the existing network, analyzing radio signal interference, and performing signal propagation testing, that you need to follow when determining the optimum installation locations for access points.
  - Chapter 16, "Installing and Configuring a Wireless LAN": This chapter explains how to plan the installation, stage the components, install the access points, and document the installation of a WLAN.
  - Chapter 17, "Testing a Wireless LAN": This chapter describes the steps and techniques necessary to test a wireless LAN, which includes signal coverage testing, performance testing, in-motion testing, security testing, acceptance testing, simulation testing, prototype testing, and pilot testing.

- Part V, "Operational Support Considerations": This part of the book includes chapters that explain what to consider when supporting an 802.11n wireless network. Readers will learn how to establish specialized support for wireless networks and perform help desk operations, network monitoring, and troubleshooting.
  - Chapter 18, "Managing a Wireless LAN": This chapter describes important operations and maintenance functions that you should consider when supporting a WLAN, including help desk, network monitoring, maintenance, engineering, configuration management, security management, trouble call coordination, operational support tools, and operational support transfer preparation.
  - Chapter 19, "Troubleshooting Wireless Networks": This chapter explains how to identify problems, such as connectivity and performance issues, and determine the underlying causes.
  - Chapter 20, "Preparing Support Staff": This chapter describes what you should consider when evaluating the experience and education of staff for supporting a wireless LAN.
- Glossary: The glossary describes terms that this book uses.

Hands-on Exercises

As mentioned in the "Goals and Methods" section, this book includes exercises that make use of free and inexpensive tools that help you gain practical experience with concepts described in the chapter. You can find these exercises on the following pages:

- Chapter 6:
  - Hands-on Exercise: Observing 802.11 Dynamic Rate Shifting—141
  - Hands-on Exercise: Observing 802.11 Active Scanning—150
  - Hands-on Exercise: Observing the 802.11 Connection Process—154
  - Hands-on Exercise: Observing 802.11 Beacons—169
  - Hands-on Exercise: Observing 802.11 Frames Resulting from Typical User Traffic—175
- Chapter 7:
  - Hands-on Exercise: Understanding Performance Impacts of Increasing 802.11n Spatial Streams—192
  - Hands-on Exercise: Understanding Performance Impacts of 802.11n Channel Bonding—193
- Chapter 11:
  - Hands-on Exercise: Analyzing Impacts on Range Using Different Data Rate Settings—305

Chapter 11

Range, Performance, and Roaming Considerations

This chapter will introduce you to:

- Range Versus Performance
- Range Considerations
- Performance Considerations
- Roaming Considerations

When designing a wireless LAN (WLAN), take care to ensure that the WLAN will satisfy requirements for signal coverage, performance, and roaming. Problems related to these items often crop up when supporting a WLAN, generally due to designers not considering all relevant elements of the design. This chapter provides insight and addresses important elements you should consider to avoid these problems.

Range Versus Performance

It would be great if WLANs had unlimited range and performance. If this were true, the job of designing a WLAN would be much easier. There would be no need to consider the multitude of design elements to ensure that there was enough signal coverage and capacity for supporting your applications. Unfortunately, due to the constraints of physics, definite range and performance limits apply.

In addition, something that complicates the design is that range and performance are sometimes indirectly proportional. By increasing some design elements (for example, transmit frequency or data rate), the performance will increase but range will decrease (if all other design parameters, environment, and so on are constant). In other cases, changing design elements, such as transmit power and antenna gain, will increase performance and range. As a result, you must be familiar with how changing various design elements impacts range and performance to design an effective WLAN.

In addition, ensure that you have a solid understanding or the WLAN requirements dealing with performance, signal coverage, and the operating environment before getting started with the design. You will need to know this to determine which elements are most important and worthwhile to change.

Note The associated data rate between a client radio and an access point generally increases as the client radio becomes closer to the access point, which results in higher throughput closer to the access point.

Range Considerations

To satisfy signal coverage requirements, you will need to install access points in optimum locations based on the results of a wireless site survey, as explained in Chapter 15, "Performing a Wireless Site Survey." This involves completing propagation tests that determine the range of the access points based on specific minimum signal levels sufficient to support required client devices and applications. 802.11n systems provide much better range and performance than legacy 802.11b and 802.11g networks, but there is fine-tuning that you can do. To maximize range and reduce the total number of access points, carefully consider the following design elements:

- Signal coverage requirements
- Radio frequency bands
- Transmit power settings
- Transmission channel settings
- Data rate setting
- Antennas
- Amplifiers
- Repeaters
- Physical obstacles
- Radio signal interference

Signal Coverage Requirements

Review requirements that define the environment where the WLAN will operate and areas where signal coverage is needed. This will give you a feel for the importance of maximizing the range. If the WLAN must provide signal coverage over a large open area where it is not feasible to install access points, for example, the use of higher-gain antennas and possibly amplifiers may prove worthwhile.

Note For details explaining how to determine signal coverage requirements, see Chapter 9, "Defining Requirements for a Wireless LAN."

Radio Frequency Bands

As part of the design, you can choose to use 2.4-GHz or 5-GHz (or both) 802.11n bands. Communications theory explains that (with all other things constant), an increase in transmission frequency causes a decrease in range of the signal. As a result, the higher transmit frequencies of the 5-GHz band should provide shorter range than the lower 2.4-GHz band. In practice, the use of 5-GHz 802.11n, though, might or might not provide shorter range. In fact, sometimes a 5-GHz 802.11n system provides the same or even greater range as compared to a 2.4-GHz system. This might occur, for example, if the noise in the 2.4-GHz band is considerably higher than in the 5-GHz band (which is often the case). The resulting signal-to-noise ratio (SNR) values of the 5-GHz system, despite a decrease in signal strength due to higher operating frequencies, might be higher due to much less noise in the 5-GHz band.

Figure 11-1 illustrates a case where the range of a 2.4-GHz and 5-GHz access point are the same. At the client device (laptop) associated with the 2.4-GHz access point, the signal level is –70 dBm, and the noise is –85 dBm. This results in a SNR of 15 dB, which of course indicates a specific level of performance. Because of higher operating frequency, the signal at the client device associate with the 5-GHz access point is significantly lower at –80 dBm (an arbitrary number chosen for illustration purposes only). Because of the much lower noise level (–95 dBm) in the 5 GHz band, the SNR for the 5-GHz system is also 15 dB, which would likely provide similar performance as the 2.4-GHz system. This indicates that the 2.4-GHz and 5-GHz systems have the same range, which is a probable outcome depending on difference in noise levels between the 2.4-GHz and 5-GHz bands. Therefore, be certain to take into account the actual environment where the WLAN will operate choosing 2.4-GHz or 5-GHz bands based on range requirements and expectations.

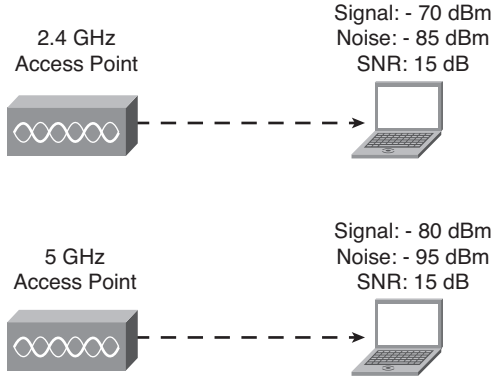

Figure 11-1 *A Case Where the Range Is the Same for a 2.4-GHz and 5-GHz System*

Transmit Power Settings

For a constant performance levels, increasing the transmit power of an 802.11 radio increases range. As the transmit power increases, communications at a particular data rate, such as 12 Mb/s, will be possible at greater ranges. The reason for this is that increasing transmit power improves the SNR at points farther away from the radio. The range expands to cover areas where increases in the transmit power causes the SNR at points farther away to be at or above the minimum signal values needed to for reliable operation. This higher SNR allows the end radios to receive communications at these farther points where they might not have been able to before.

Figure 11-2 illustrates this point. With the access point tuned to 10 dBm, the SNR at Location A is 15 dB, which for this example we will assume is the signal strength necessary for reliable communications at 12-Mb/s data rates. At Location B, the signal level is –76 dBm due to free space loss, attenuation, and so on, which results in a 9 dB SNR. Therefore, at Location B, the access point tuned to 10 dBm will support something less than 12 Mb/s. If you increase the access point transmit power to 16 dBm (a 6 dB increase), the signal level at Location B will increase by 6 dB to –70 dBm. This makes the SNR at Location B equal to 15 dB, which allows reliable 12-Mb/s operation. As a result, increasing the transmit power has made it possible to extend the range for a specific data rate.

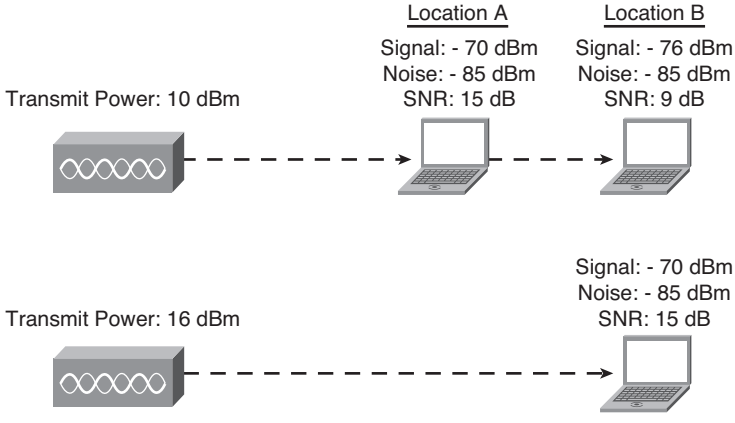

Figure 11-2 *Transmit Power Increases Provide Greater Range by Increasing Signal Strength*

This increase in range, however, only impacts the communications in one direction, which is the outward path relative to the radio with increased transmit power. The increase of transmit power of an access point, for example, only improves the range of the communications path from the access point to the client radios. To improve the overall communications of 802.11 signals, which occur in both directions between the access point and client radios, you will need to increase the transmit power of the client radios as well. In fact, it is usually not useful to increase the transmit power of the access points because the client radios are almost always operating at much lower transmit power. As a result, it

will likely only be worthwhile to increase the transmit power of the client radios. The signals going from the access points to the client radios are already relatively strong. The increase in client radio transmit power alone will improve the range of the overall communications in this case.

An advantage of using transmit power changes to improve range is that there are no expenses for additional hardware. A problem, however, is that it might not be possible to increase the transmit power on the client radios (the devices that would likely need a boost in power) because they might already be set by default to the highest power. Also, if you have little control over the client devices operating on the network, such as the case with public networks, you might not have the ability to change the transmit power of some or all the client radios.

Note Some WLAN vendors may have proprietary features where the client radios automatically change to a specific transmit power based on the data rate set in the access point.

Transmission Channel Settings

Within each of the 802.11 frequency bands, specific operating channels span from the lower-frequency end of the band to the higher-frequency end of the band. These channels use different transmission frequencies, but there negligible impact on range from using the lower-frequency channels versus the higher-frequency channels based on the theory that increases in frequency causes shorter range (and vice versa). For example, choosing channel 1 versus channel 11 in the 2.4-GHz band has no significant impact on range. There is not enough spread in the frequencies across the band to make a notable difference in range.

The choice of transmission channel settings does, however, make a difference on range if it is possible to choose a channel to avoid radio signal interference. An access point, for example, may be set to channel 11, but you might notice from a spectrum analyzer that there is significant interference in the upper part of the band (including channel 11). The lower part of the band, channels 1 through 3, may be relatively free from interference. By changing the access point to channel 1, it is possible to improve the SNR throughout the area, which improves range. For example, the noise levels relative to channel 1 might be 6 dB lower than what it had been for channel 11. As a result, the signal level can be 6 dB lower and still constitute acceptable SNR. Figure 11-3 illustrates this concept.

As with transmit power, changing the transmission channel to improve range does not cost anything in terms of new hardware. In addition, with infrastructure WLANs (ones with access points), there is no need to make changes to client radios. As a result, transmission channel changes can be made on networks where you may have little or no control over the client radio settings. Keep in mind, however, that there is a limit of nonoverlapping channels available (especially in the 2.4-GHz band) and radio signal interference may change over time. For example with larger WLANs, you might have significant inter–access point interference if you only set access points to lower-frequency channels to avoid the interference present in the higher-frequency channels.

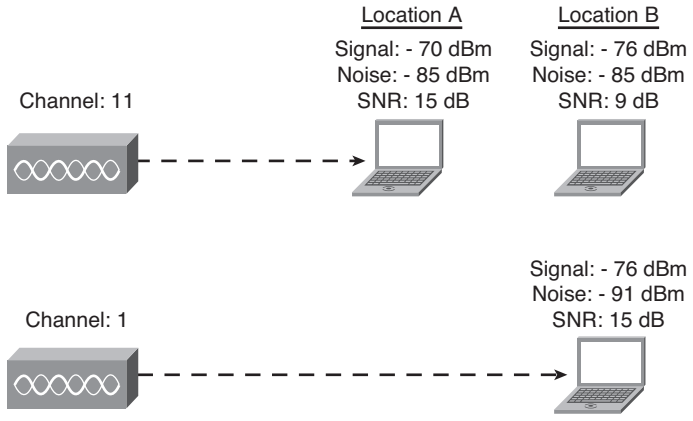

Figure 11-3 *Transmission Channel Changes Can Provide Greater Range by Lowering Noise Levels*

Data Rate Settings

At first, it may seem that data rate settings only impact the performance of a WLAN. The data rate settings, however, has an indirect impact on range. As a general rule (with everything else constant), an increase in data rate causes a decrease in range. Therefore, data rate and range are indirectly proportional. The reason for this is that higher data rates require higher received signal strength at the radio for the receiver to decode the 802.11 signal. Companies that make access points and client radios publish the received signal strength that supports various data rates.

As a result, be careful when adjusting the data rate in access points and client radios. By default, access points and client radios usually have their data rate setting configured as "auto" so that they will rate shift as needed to maintain associations with users. This is usually the best setting for general usage. Most access points also allow the data rate to be set to specific values, such as 12 Mb/s. If it is desirable to maximize range, consider setting all access points and client radios to low data rates. Just be sure that data rates are set high enough to provide adequate levels of performance.

Something to realize is that the setting in the access point only applies to the data rate that the access point uses, not the wireless clients. For example, setting the access point to 54 Mb/s causes the access point to transmit all data frames at 54 Mb/s. In this situation, wireless clients set to auto still continue to use higher data rates if possible. To extend range by forcing lower data rates, set both access points and user radio cards to the lower data rate configurations. That ensures that the data rates are the same in both directions.

Note Some WLAN vendors may have proprietary features where the client radios automatically change to a specific data rate based on the data rate set in the access point.

Hands-On Exercise: Analyzing Impacts on Range Using Different Data Rate Settings

This exercise allows you to experience the impacts that different date rate settings have on range between a client device and an access point. While observing the connection status of a wireless client device and an access point, you will determine the maximum range that provides a connection at different data rates.

Perform the following steps:

Step 1. Obtain test equipment. You will need a wireless client device and an access point to complete this exercise.

Step 2. Disable adaptive transmit power control on the access point if applicable.

Step 3. Associate the client device with the access point, with the access point and client radio configured for the maximum fixed data rate.

Step 4. Initiate a continuous TCP/IP ping between the client device and the access point to generate regular traffic between the client radio and the access point. This is necessary for the client radio to accurately monitor the connection state of the client radio.

Step 5. Position the client device close to the access point and begin walking away from the access point with the client device along a defined path until the connection is lost.

Step 6. Observe the connection state as you walk away from the access point until the connection is lost. You can observe this in the Windows (or vendor-specific) wireless client utility or by monitoring the continuous pings. If the pings continue successfully, the connection status is "connected." If the pings discontinue, the connection status is "disconnected."

Step 7. Note the location/range of where the connection was lost.

Step 8. Repeat Steps 5 and 6 multiple times with the access point and client radio configured to progressively lower fixed data rates. For example, after performing the test with the higher data rate setting, you might want to perform a second test by choosing a data rate somewhere in the middle between the lowest and highest data rate. As a third test, you could set the access point and client radio to the lowest fixed data rate. In each test at a different data rate, note the range along the predefined path where a connection is lost. What differences in range do you see for the various data rate settings?

As you lower the data rate settings, the range should increase where the connection is lost between the access point and the client device. The reason for this is that, as explained earlier, 802.11 radios have better receive sensitivity at lower data rates, which allows the radios in the client device and access point to be farther apart.

Antennas

The factory-default antennas that come with an access point usually have low gain (around 2dB). If the access point has removable antennas, replacing the default antennas with higher gain omnidirectional or directional antennas boosts range. For example, replacing a standard 2 dBi antenna with a 6 dBi omnidirectional antenna effectively adds 4 dB to the signal strength throughout the coverage area. As shown in Figure 11-4, the result of adding this gain improves the signal strength at Location B enough to maintain 15 dB SNR as compared to only 9 dB is using the standard 2 dBi antenna. Therefore, the increase in antenna gain has provided greater range for a specific data rate that corresponds to 15 dB SNR.

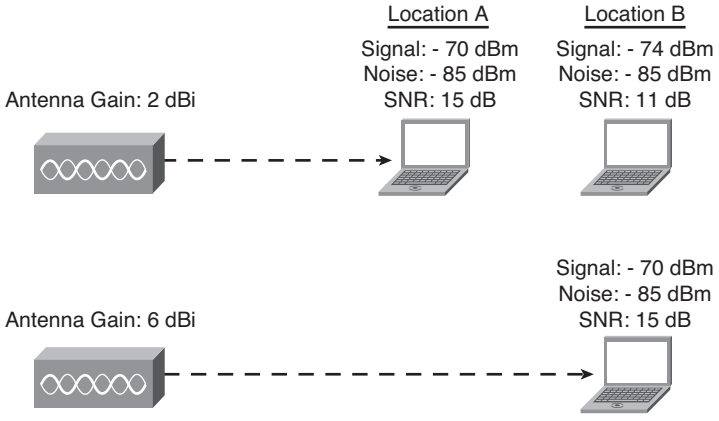

Figure 11-4 *Higher-Gain Antennas Boost Range by Increasing Signal Strength*

Note Keep in mind that some access points do not have removable antennas, which of course precludes you from using different antennas to increase range.

A higher-gain antenna, installed for instance on an access point, improves range from the access point to the client radio and from the client radios to the access point. This is different from increasing transmit power on only the access point, which would only increase range for the communications going from the access point to the client radios. The reason that a higher-gain antenna improves range in both directions is that the higher gain of the antenna improves both transmission and reception of radio waves. Therefore, the installation of higher-gain antennas can provide significant increases in range without making changes to the client radios.

In addition to using higher-gain antennas, antenna diversity can also help extend range in both directions because it minimizes multipath propagation. Diversity is an important part of 802.11n, and various vendors sell 802.11n access points and client radios that have

different levels of diversity. If your intent is to maximize range, choose components that have high levels of diversity.

An advantage of using higher-gain antennas or diversity is that it impacts range in both directions. As a result, you may be able to get by with changing the antenna configuration on only the access point, avoiding the need to alter each client radio. The cost of upgrading the antennas, however, might be considerable (possibly $50 to $100 or more per access point). Therefore, the cost might be prohibitive in larger networks.

Be sure to take into account different antenna gain and diversity with actual propagation testing in the target operating environment to determine the lowest overall cost of deploying the network. For example, you might find that the use of standard 2 dBi antennas may require the need for 100 access points, and the use of 6 dBi antennas may reduce the number of access points to 80. The addition costs for 6 dBi antennas in this example would probably be $4000 to $8000 ($50 to $100 each for 80 access points). This additional cost is likely much less than the 20 additional access points that you would need to purchase if going with the standard 2 dBi antennas. As a result, in this example, it would be worth the additional cost for the 6 dBi antennas. This assumes that the goal is to maximize range.

The trouble with increasing antenna gain for purposes of extending range is that you will likely place the access points farther apart (of course to reduce the number of access points and reduce costs). This results in a larger 802.11 collision domain, which limits the capacity of the WLAN. More client devices end up connecting to fewer access points.

Note For more details on antennas, see Chapter 3, "Wireless LAN Types and Components."

Amplifiers

The use of an amplifier is a way of increasing range. Similar to increasing the transmit power on the access point (or client radio) an amplifier boosts the signal strength throughout the coverage area, as illustrated in Figure 11-5. In addition, amplifiers have receive gain, which amplifies the incoming signals coming from the client devices. Therefore, the signal strength increasing behavior of an amplifier is similar to that of an antenna.

Note When using amplifiers, be certain to follow your country's regulatory rules that define the usage of radio frequency (RF) amplifiers.

Most WLAN amplifiers are rated at a specific transmit power, such as 200 mW, and a specific receive gain, such as 15 dB. Amplifiers with higher transmit power produce greater range for communications going from the access point to the client radios. The receive gain will increase the range for communications going from the client radios to the access point. Therefore, be sure to take both transmit power and receive gain of the

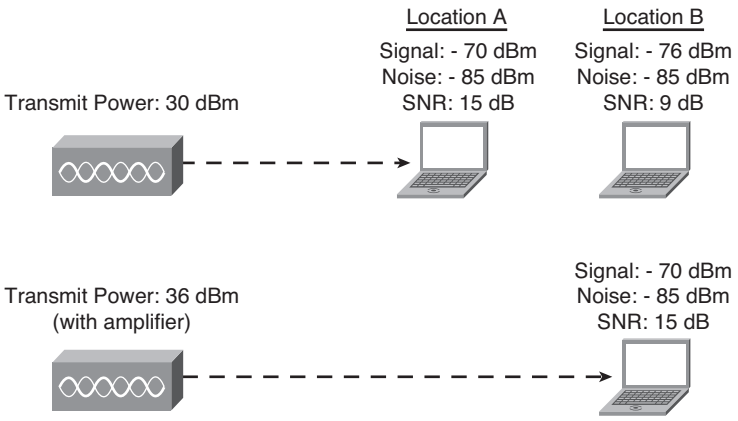

Figure 11-5 *Amplifiers Improve Range by Increasing Signal Strength*

amplifier into account when determining which one to use. Of course, as with anything else, it is always a good idea to do some propagation testing with amplifiers to realize their actual impact on range.

Companies such as Hyperlink and RF Linx sell amplifiers for WLANs. These amplifiers are designed to install between the antenna and the access point. As a result, you can use an amplifier only if it is possible to remove the access point antenna.

Note For more details on amplifiers, see Chapter 3.

Repeaters

A WLAN repeater is meant to reside between access points and client radios and regenerate signals it receives. As a result, a repeater increases range between access points and client radios (see Figure 11-6). A repeater might double the range, but it can significantly reduce the capacity of the WLAN because the repeater retransmits data frames it receives. This causes a duplication of data traffic, which reduces the overall capacity by up to 50 percent. This could be a problem if performance is important. Also, a repeater requires electrical power, which might be costly to install. Because a repeater does not connect to the distribution system, Power over Ethernet (PoE) is not an option.

Note For more details on repeaters, see Chapter 3.

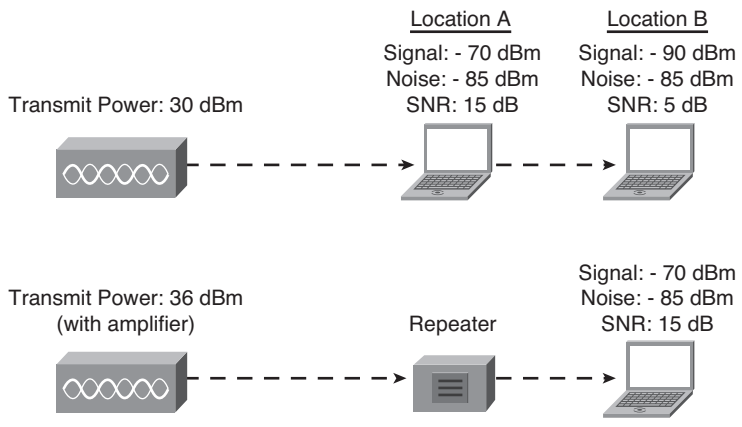

Figure 11-6 *Repeaters Extend Range Between Access Points and Client Radios*

Physical Obstacles

Certainly physical obstacles may be present within the operating environment of the WLAN, and these obstacles offer varying amounts of attenuation. To improve range in some areas, consider installing access points in locations that avoids obstacles. If possible, even consider moving some obstacles if it is advantageous (and feasible) to improve range. This effectively improves the signal strength throughout the applicable areas.

For example, signal coverage may be needed in an office where there are ceiling high filing cabinets along one of the walls in the office. These cabinets will likely highly attenuate RF signals. As a result, it would be wise to position one or more access points to cover the office so that the signals do not travel through the cabinets.

Note For more details on obstacles and RF signal propagation, see Chapter 2, "Radio Wave Fundamentals."

Radio Signal Interference

As discussed earlier in this chapter, a way of avoiding existing interference is to use frequencies where interference is less, such as using the 5-GHz frequency band or turning the access point to channels having lower interference levels. By reducing radio signal interference, you can increase range between access points and client radios, as illustrated in Figure 11-7. Another similar way of improving range is to remove the source of interference. For example, it might be possible to decrease the noise levels by 6 dB in the 2.4-GHz band by stopping the use of 2.4-GHz cordless phones (and possibly switching to 5-GHz or 6-GHz phones instead). Also you could use RF shielding to reduce noise. Special RF shielding paint and wallpaper is available that offers high degrees of attenuation (80

dB). Of course the elimination of interference sources may not be feasible, but it is at least something to consider.

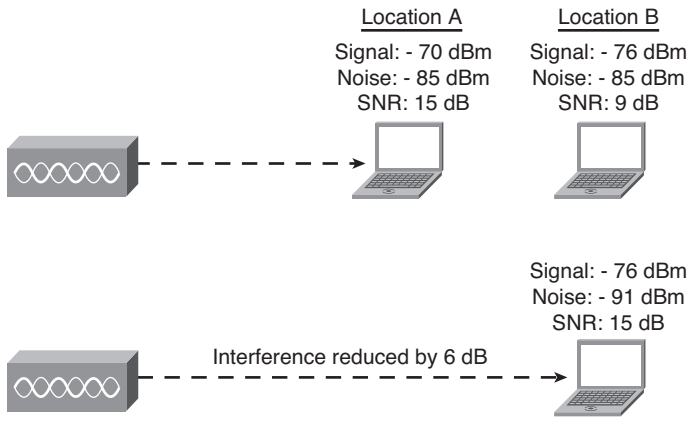

Figure 11-7 *Lowering Radio Signal Interference Increases Range*

Note For more details on radio signal interference, see Chapter 4, "Wireless LAN Implications."

Extending Municipal Wi-Fi Mesh Indoors

Most municipalities require Wi-Fi signal coverage in 90 percent of outdoor areas and 70 percent inside homes and businesses. For indoor places, the coverage is generally required just inside the exterior wall the facility on the first and second floors. To meet overall coverage requirements, the trend is to install Wi-Fi mesh nodes on city-owned assets, such as streetlamp poles and traffic lights. This generally offers good coverage outside throughout the city, but indoor coverage is generally not sufficient without careful planning.

Indoor signal propagation suffers because the exterior walls of the facilities offer significant attenuation. In addition, the transmit power of user devices operating inside the buildings is usually relatively weak. The transmit power of the mesh nodes is much higher, but this only affects the downlink communications path, from the mesh node to the user device. This does not do much good when the user devices have much lower transmit power. In this case, the ability for the communications link to operate is based on the weaker uplink signal, which causes limited range.

Because of varying wall attenuation and relatively weak transmit power of user devices operating inside the facilities, signal propagation indoors is not reliable and difficult to verify. You cannot depend on getting inside an appropriate sample of these facilities to test signal propagation and tweak the positioning of the mesh nodes to improve coverage.

Most of the indoor locations are private homes and businesses, and a large number of them are not likely going to let you in to do testing.

As a result, when designing a municipal Wi-Fi network, it is highly recommended to specify the use of indoor customer premises equipment (CPE), which offers a stronger uplink signal to compensate for the attenuation of the walls. The use of indoor CPE will make signal coverage inside buildings much more reliable and satisfy requirements. I have found that about 50 percent of the homes and businesses in cities actually require CPE to provide acceptable indoor coverage, but a blanket requirement for all indoor locations to use CPE may be beneficial.

CPE installs inside the facility, near one of the exterior walls, and associates via Wi-Fi to the nearest mesh node. CPE also provides a separate Wi-Fi or Ethernet connection inside the facility. If it is Wi-Fi, users will likely have much greater indoor Wi-Fi coverage than what the municipal network requirements specify. Each indoor location will have the equivalent of a Wi-Fi router installed inside the building. If it is Ethernet, users will need to connect a laptop or PC directly to the CPE device or plug in an external Wi-Fi router or access point.

Something to keep in mind is to properly set user expectations regarding indoor coverage of a wireless municipal network and the need for CPE. Many potential users are accustomed to using Wi-Fi hotspots where signal coverage is good without CPE devices. A municipality can circumvent frustrated users by educating users early on during the deployment of the network. Users need to realize that without indoor CPE, they will not have reliable Wi-Fi signal coverage.

Performance Considerations

When WLANs first became available in the early 1990s, primary applications were wireless bar code solutions for needs like inventory control and retail price marking. Data transfers for these types of applications do not demand very high performance. In fact, 1 Mb/s data rates are generally sufficient to handle the transfer of relatively small bar codes for a limited number of users.

Today, enterprises are deploying WLANs for larger numbers of users with needs for corporate applications that involve large file transfers and wireless telephony. In addition, there are often needs for supporting a high density of users in a smaller area, such as a conference room. The need for higher data rates and techniques to improve performance of WLANs is becoming crucial to support these types of applications. To get that extra performance when designing a WLAN, consider the following elements:

- Throughput versus data rate
- Radio frequency bands
- Transmit power settings
- Transmission channel settings

- Data rate settings
- Antennas
- Amplifiers
- Obstacles
- Radio signal interference
- Channel width settings
- Signal coverage
- Fragmentation settings
- Request-to-send / clear-to-send (RTS/CTS) settings
- Multicasting mechanisms
- Microcell deployment strategies

Throughput Versus Data Rate

The data rate of a signal is based on the time it takes to send information and overhead data bits when transmitting. Therefore, the aggregate data rate (throughput) is actually much lower because of delays between transmissions. Data rate mostly affects the delay performance of a WLAN. The higher the data rate, the lower the delay when sending data from one point to another. As a result, higher data rates can increase the capability to support a larger number of users. Data rate alone is not a good measure for the performance of the system, though. You also need to consider the effect of overhead bits, waiting times to access the medium, and the format of the data being sent.

Actual throughput is a much better indicator of the performance of a WLAN because it provides an indication of the time it takes to send information. Throughput is the flow of information over time. It is important to not confuse throughput with 802.11 data rate, which is the speed that the data bits in individual 802.11 data frames are sent. Because there is idle time between 802.11 data frames and retransmission due to noise, the throughput is always less than the data rate. Throughput, however, provides a more accurate representation of the delays that users experience because they are concerned with how fast information is sent, not 802.11 frames. It is possible to have a very high 802.11 data rate and still have throughput that is relatively low. This can occur, for example, when the user is close to an access point but there are many other users actively accessing the WLAN from the same access point or if there is substantial radio signal interference present. In these cases, the WLAN carries the information at a much slower rate. As a result, be sure to focus on specifying throughput, not 802.11 data rates as the basis for performance.

Note When laptops are unplugged from an electrical outlet and running on batteries, the client device operating system will likely cause an 802.11n client radio to enter power-saving mode. As a result, throughput may drop by as much as 50 percent. To ensure throughput is not affected when running on batteries, configure the operating system to not invoke client radio power management.

Radio Frequency Bands

As mentioned earlier in this chapter, you can choose to use 2.4-GHz or 5-GHz (or both) 802.11n bands. In addition to the impact this selection has on range, the choice of frequency band also affects performance. The 5-GHz band includes much more spectrum (and corresponding channels) as compared to the 2.4-GHz band. There are many more overlapping channels in the 5-GHz band as compared to the 2.4-GHz band. In addition, the 5-GHz band is usually relatively free from RF interference sources. As a result, the 5-GHz band offers much greater capacity. Keep in mind, however, that the 5-GHz band, as explained earlier, might provide less range as 2.4-GHz deployments.

Transmit Power Settings

For a constant range, increasing the transmit power of an 802.11 radio increases performance in the outward direction. As the transmit power increases, communications at a particular location will be possible at greater data rates. The basis for this is that increasing of transmit power improves the SNR at a particular location, which allows the receiving radio to decode signals at higher data rates.

For example, as shown in Figure 11-8, increasing the transmit power of the access point by 6 dB causes a 6 dB increase in the signal strength and corresponding SNR throughout the coverage area. In the case shown in Figure 11-8, the client device associated with the access point set to higher transmit power has a SNR of 21 dB, which is significantly higher than it would be if the transmit power of the access point were set to a lower level. The higher signal level (and SNR) allows the client device to receive 802.11 signals at higher data rates.

This increase in data rate applies to the communications in only one direction, which is the outward path relative to the radio with increased transmit power. The increase of transmit power of an access point, for example, only improves the data rate of the 802.11 data frames being sent from the access point to the client radios. To improve the overall communications of 802.11 signals, you may need to increase the data rate settings on the access points and the client radios. As discussed previously in this chapter, client radios may have considerably less transmit power as the access points. Therefore, you will likely need to increase the transmit power on the client radios to see any improvement in data rates.

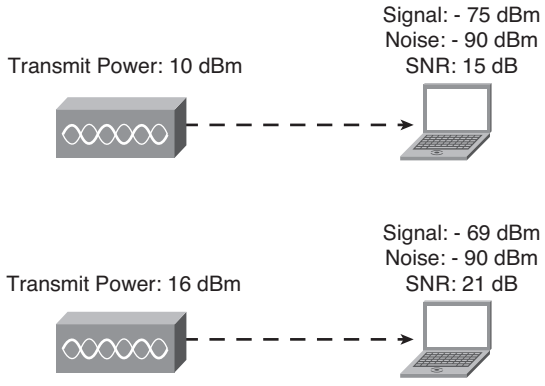

Figure 11-8 *Transmit Power Increases Provide Higher Data Rates at Specific Points Due to Corresponding Increases in SNR*

Transmission Channel Settings

As with range improvements, transmission channel settings can impact performance as well if it is possible to select a channel that avoids radio signal interference. Figure 11-9 illustrates an example of this concept, where testing has shown that the noise level for channel 1 is 5 dB lower than the noise level for channel 11. Because of the lower radio frequency interference corresponding to channel 1, the resulting SNR for channels at the client device is 15 dB, which enables the applicable client radio to process 802.11 signals at a higher data rate.

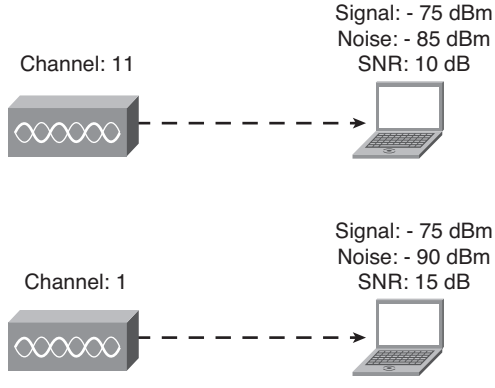

Figure 11-9 *Transmission Channel Changes Can Provide Greater Performance by Lowering Noise Levels*

Data Rate Settings

If you need to deploy a high-performance WLAN, consider configuring data rate settings to higher fixed values. This forces operation at a higher specific data rate and avoids transmissions at lower data rates, which would negatively impact overall performance. Just keep in mind, however, that using higher data rate settings will significantly reduce range. Also, as explained earlier in this chapter, data rate settings impact communications in only one direction. For example, setting the access point to 54 Mb/s causes the access point to transmit all data frames at 54 Mb/s, but the client radios may be transmit at different data rates depending on their data rate settings. As a result, you must configure the data rate settings in client radios (which might not be feasible) to realize benefits of using higher fixed data rate settings to improve performance.

Note Check administration logs to verify that client devices are connecting to the network at desired 802.11n rates.

Antennas

The use of higher-gain antennas increases communications performance in both directions between access points and client radios. For example, as Figure 11-10 illustrates, if you replace a standard 2 dBi antenna with one having 6 dBi, the signal level and corresponding SNR at the client radio at a specific location will increase. The higher signal level and SNR allows the radio in the access point and client radio to decode signals at higher data rates. A higher degree of antennas diversity has a similar affect on performance. Similar to using higher-gain antennas or diversity to improve range, be sure to take into account different antenna gain and diversity with actual propagation testing in the target operating environment to determine the lowest overall cost of deploying the network.

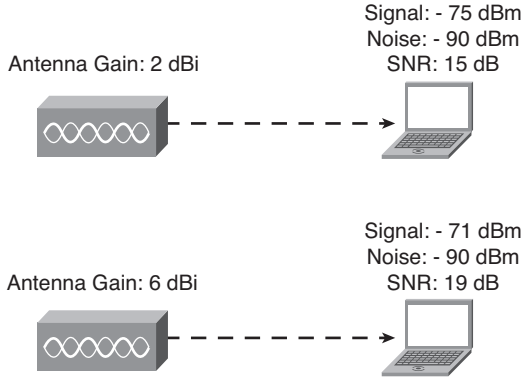

Figure 11-10 *Higher-Gain Antennas Boost Performance Throughout the Coverage Area*

Amplifiers

In addition to improving range, an amplifier can also increase performance. Because an amplifier increases the signal strength and corresponding SNR throughout the coverage area, a client radio at a specific point is able to decode the 802.11 signals at a higher data rate. For example, as shown in Figure 11-11, without an amplifier at the access point, the signal strength and SNR at the client device is -75 dBm and 15 dB, respectively. After installing an amplifier on the access point, the signal strength and SNR at the client device increase to –69 dBm and 21 dB, respectively. As a result, in this example, the client radio is able to support reception of data frames at a higher rate than without the amplifier because of the higher signal level and SNR. Also for similar reasons, because the amplifier's receive gain, the access point will also be able to receive 802.11 signals from the client radio at a higher data rate.

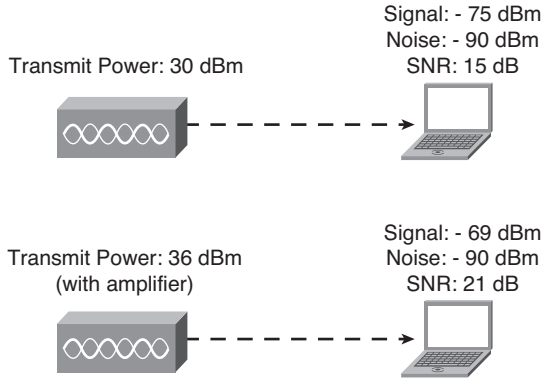

Figure 11-11 *Amplifiers Improve Performance Throughout the Coverage Area*

Radio Signal Interference

By reducing radio signal interference, it is possible to increase performance at specific points within the coverage area. For example (see Figure 11-12), a reduction of noise levels by 6 dB (possibly by eliminating the operation of other radio equipment) will raise the SNR at points throughout the coverage area by 6 dB. This enables the access points and client radios to successfully decode 802.11 signals at higher data rates.

Channel Width Settings

The 802.11n standard provides two different channel width settings, 20 MHz and 40 MHz. The wider 40-MHz channels support much higher performance as compared to 20-MHz channels. For 2.4-GHz implementation, however, it is not wise to configure 40-MHz channels. As discussed in other parts of this book, there is not enough spectrum in the 2.4-GHz band to support multiple 40-MHz channels without significant inter–access

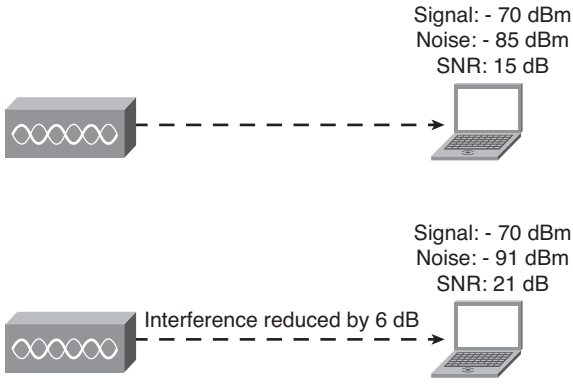

Figure 11-12 *Lowering Radio Signal Interference Increases Performance at Specific Locations*

point interference. As a result, if you choose to implement the 2.4-GHz band, the only practical option is 20-MHz channels.

The 5-GHz band, however, has a much greater amount of spectrum, with plenty of room for 40-MHz channels. Therefore, seriously consider configuring the network for 40-MHz channels. To accommodate 40-MHz channels, the client radios must be 802.11n-compliant. As a result, it might not be possible to implement 40-MHz channels if the network must accommodate legacy (802.11b and 802.11g) client devices. A way of still taking advantage of 40-MHZ channels in this case, as expressed in other parts of this book, is to configure legacy radios to connect to the WLAN over 2.4 GHz (with 20-MHz channels) and have only 802.11n devices connect via 5 GHz (with 40-MHz channels).

Signal Coverage

As the basis for providing good performance, it is important to have adequate signal coverage throughout the required coverage areas. In areas that have weak signal coverage, the signal level and corresponding SNR will be relatively low. The 802.11 radios might still be able to decode the signals and successfully communicate, but the data rate may be fairly low. To ensure that signal coverage is good enough, perform a proper wireless site survey as described in Chapter 15.

Fragmentation Settings

The use of 802.11 fragmentation can increase the reliability of 802.11 data frame transmissions in the presence of radio frequency interference, which improves the throughput of the network. Because of sending smaller frames, corrupted bits in the frame due to radio frequency interference are much less likely to occur. If a frame does receive corrupted bits, the source station can retransmit the frame quickly.

The fragment size value can typically be set manually on access points and client radios between 256 and 2048 bytes. This value is user controllable. In fact, you activate fragmentation by setting a particular frame size threshold (in bytes). If the frame that the access point is transmitting is larger than the threshold, it will trigger the fragmentation function. If the packet size is equal to or less than the threshold, the access point will not use fragmentation. Of course, setting the threshold to the largest value effectively disables fragmentation.

A good method to find out whether you should activate fragmentation is to monitor the WLAN for retransmissions. If very few retransmissions are occurring, do not bother implementing fragmentation. The additional headers applied to each fragment will likely dramatically increase the overhead on the network, which will actually reduce throughput. If you find a relatively high percentage of retransmissions (greater than 5 percent) and the presence of radio signal interference or weak signal levels is likely causing the retransmissions, try using fragmentation. This can improve throughput if the fragmentation threshold is set to the optimum value, which is where the throughput is maximum.

If the retransmission rate is relatively high, start by setting the fragmentation threshold to around 1000 bytes, and then tweak it until you find the best results. After invoking fragmentation, follow up with testing to determine whether the number of collisions is less and that the resulting throughput is better. You should try a different setting or discontinue using it altogether if the throughput drops (even if you have fewer retransmissions).

The issues with using fragmentation to improve performance is that interference driving the retransmission rate may change over time or as users roam throughout different portions of the signal coverage area. On one day, for example, the presence of significant radio signal interference may cause the retransmission rate to be around 20 percent. In this case, you may find that a fragmentation threshold of around 800 bytes maximizes throughput. On another day, the interference may go away, resulting in a drop in the retransmission rate to only 1 percent or 2 percent. Without changing the fragmentation threshold, throughput may actually drop because the cost of additional overhead resulting from the fragmentation mechanism is not providing much benefit of reducing the retransmission rate.

Note For more details on the 802.11 fragmentation mechanism, see Chapter 6, "IEEE 802.11 Medium Access Control (MAC) Layer."

RTS/CTS Settings

The use of 802.11 RTS/CTS can increase the reliability of 802.11 data frame transmissions in the presence of hidden nodes, which improves the throughput of the network. Similar to analyzing the need for fragmentation, a way to gauge whether RTS/CTS will help throughput is to monitor the WLAN for retransmissions. If the retransmission rate is low (under 5 percent), do not implement RTS/CTS. The additional frame transmissions need to implement RTS/CTS will likely dramatically increase the overhead on the network, which will actually reduce throughput.

If the retransmission rate is high, and you find a large number of collisions with users that are relatively far apart and likely out of range of each other (that is, hidden nodes are present), try enabling RTS/CTS on the applicable client radios. After activating RTS/CTS, test to determine whether the number of retransmissions is less and the resulting throughput is better. Because RTS/CTS introduces overhead, disable it if you find a drop in throughput, even if you have fewer collisions. After all, the goal is to improve performance.

Of course, keep in mind that user mobility can change the results. A highly mobile user may be hidden for a short period of time, perhaps when you perform the testing, then be closer to other stations most of the time. If retransmissions are occurring between users within range of each other, the problem may be the result of radio signal interference. In that case, fragmentation might help.

In most cases, initiating RTS/CTS in the access point is fruitless because the hidden station problem does not exist from the perspective of the access point. All stations having valid associations are within range and not hidden from the access point. Forcing the access point to implement the RTS/CTS handshake will significantly increase the overhead and reduce throughput. Focus on using RTS/CTS in the client radios to improve performance.

Note For more details on the 802.11 RTS/CTS mechanism, see Chapter 6.

Bandwidth Control Mechanisms

To provide consistent performance for all users, it might be necessary to implement bandwidth control mechanisms, which divides the total capacity of the network into smaller sizes made available to each user. For example, as shown in Figure 11-13 (case without bandwidth control), a single user (client device A) may download a very large file that requires a few minutes (or even hours), consuming nearly all the capacity of the network. As a result other users, such as client B and C may have very little if no throughput. This uncontrolled use of the network can aggravate users and significantly reduce the effectiveness of the network. A solution to this is to use bandwidth control and configure the access points (or other applicable components) to provide each user a throughput limit, such as 250 kbps each. This level of performance, based on the total users and utilization of the network, forces users to share the total capacity of the WLAN in a manner that ensures sufficient performance for everyone.

Microcell Deployment Strategies

If WLAN requirements call for extremely high performance, consider using a high density of access points. This calls for turning down the transmit power of all access points and client radios, which forces access points to be much closer together (and avoid interfering with each other). This “microcell” architecture makes the physical area collision domains smaller than with conventional access point density. The microcell architecture leads to much higher performance because there are fewer client devices connecting to

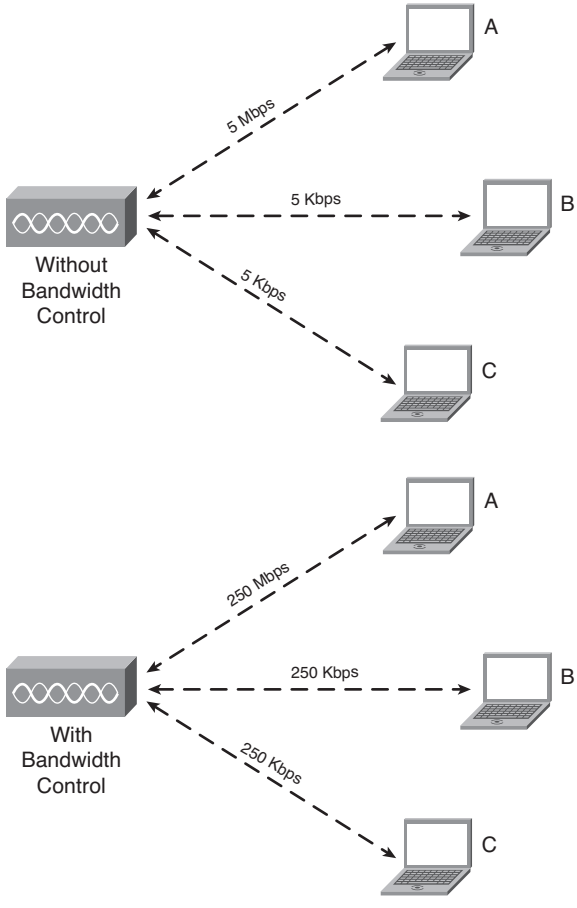

Figure 11-13 *Bandwidth Control Provides Consistent Performance for All Users*

each access point. This allows each client device radio to consume a greater percentage of the access point's capacity and avoid collisions with other radios. Therefore, performance can be much greater.

An issue with using higher access point density to improve performance is that it leads to a great number of access points. Of course this means that the deployment will cost more, possibly considerably more. To reduce the need for increasing the density of access points, first consider all other less-expensive options covered previously in this chapter.

Note Your organization will likely not realize the true potential of 802.11n until you are able to migrate away from legacy (802.11b and 802.11g) devices and implement a pure 802.11n network. Of course, this requires that all wireless client devices must implement 5-GHz frequencies.

Determining Wireless LAN Capacity

One way of sizing up a WLAN is to install the access points and see what happens. This approach does not require much investment in time and brainpower; however, you may never really know the maximum capacity until users start to complain. For example, you may install a WLAN to enable users in an office to access Internet services. After first commissioning the system, only a handful of users may be active at any given time. Within 6 months, the number of active users may increase to 50, and you start to observe users complaining about slow performance. This is an indirect sign that access points are operating at capacity. Of course, this result assumes that there are no other bottlenecks, such as sluggish servers or slow Internet service provider (ISP) connections.

Another method of sizing a WLAN is to gather up a bunch of people armed with wireless client devices and have them hammer on the network. Just keep adding more and more active users until performance starts to decline to a level that is not acceptable. The maximum capacity could be the point at which users experience more than five seconds delay when loading a particular web page, for example. This approach will provide fairly accurate results, but it is often not feasible. The difficulty is finding enough people and client devices to perform the testing. In most cases, this type of testing is just too expensive.

Simulation programs, such as OPNET, run on a computer and imitate a WLAN under different situations. With simulation, you can artificially characterize WLAN components, such as access points, client radios, and users. A simulation calculates resulting throughput, which gives you a good idea of how many users can be active on the network. By adjusting the number of users, you can estimate how many users that access points can handle and the resulting per user performance. A strong advantage of simulation is that it can be done before purchasing and installing the WLAN. Simulation tools are rather costly, however, with prices in the tens of thousands of dollars. In addition, you will probably have a steep learning curve before being proficient at developing the simulation models. This can make the simulation option out of reach for most companies. Results are also only as good as the utilization level estimates.

Roaming Considerations

WLAN requirements generally call the ability of users to roam with wireless client devices throughout the coverage area. Each client radio will roam differently, depending on proprietary protocols that the vendor has incorporated into the radio. The type of wireless application that the client device is using also impacts the ability to roam. As a result, it is crucial that you test the roaming capability of all client device before finalizing the design of the WLAN.

When designing a WLAN, consider the following elements that impact roaming:

- Roaming levels
- Wireless IP phone roaming
- Mobility settings

Roaming Levels

As a basis for designing a WLAN that provides effective roaming, it is important to first understand basic roaming concepts. For WLANs, roaming takes place at several levels. As shown in Figure 11-14, roaming can take place at Layer 2 or Layer 3. As a user moves about the coverage area, the client radio automatically hands off from one access point to another as needed to support communications. This is Layer 2 roaming, sometimes referred to as access point roaming. In addition, the client device might need to roam from one subnet to another, which is Layer 3 roaming.

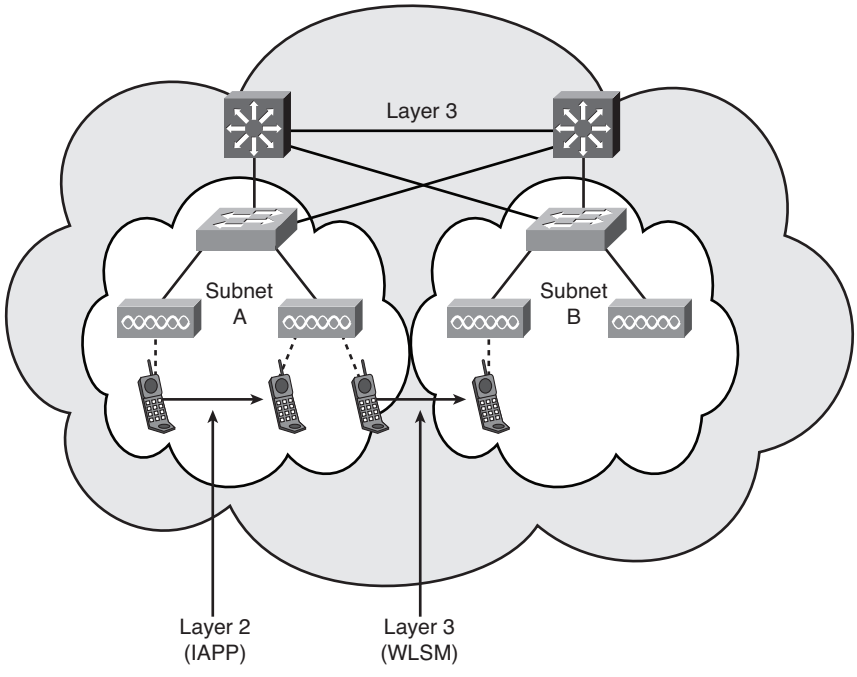

Figure 11-14 *Layer 2 Versus Layer 3 Roaming*

Access Point Roaming

Through the collaboration of WLAN vendors, the Inter–Access Point Protocol (IAPP) specification provides a common roaming protocol enabling users (client radios) to move throughout a facility while maintaining a connection to the network via multivendor access points. Interoperability tests and demonstrations show that IAPP works with a variety of access points. The Wi-Fi Alliance includes interoperable roaming as a requirement to receiving Wi-Fi certification.

The IAPP specification builds upon the capabilities of the IEEE 802.11 standard, using the distribution system interfaces of the access point that 802.11 provides. IAPP operates between access points, using the User Datagram Protocol (UDP) and the Internet Protocol (IP) as a basis for communications. IAPP defines two basic protocols: the

Announce Protocol and the Handover Protocol. The Announce Protocol provides coordination between access points by performing the following functions:

- Informs other access points about a new active access point
- Informs the access points of networkwide configuration information

The Handover Protocol informs an access point that one of its stations has reassociated with a different access point. The old access point forwards buffered frames for the station to the new access point. The new access point then updates filter tables to ensure that MAC-level filtering (bridging) will forward frames appropriately.

The finalization and proliferation of IEEE 802.11r and 802.11k amendments to the 802.11 standard have positive impacts on access point roaming. 802.11r provides seamless roaming between access points. The main application for 802.11r is for providing effective roaming for VoIP and security mechanisms. 802.11r provides functions for determining QoS and performing security protocol handshakes before handoffs occur to avoid delays after handoff. 802.11k works in conjunction with 802.11r by providing information to discover the best available access point for handoff purposes. Consider incorporating 802.11r and 802.11k into VoIP and security applications.

Subnet Roaming

As a wireless client device roams from one IP subnet to another, the client device might need to obtain a valid IP address for the new subnet. The client device can make use of DHCP to obtain the IP address, but this is not always effective when supporting mobility. DHCP is not designed to renew addresses when crossing subnet boundaries. As a result, it might be necessary to configure a WLAN to operate on a single subnet.

This might work in a private network, but the subnet roaming issue resurfaces when the client device needs to roam to another network. Consider the use of wireless middleware for applications that are affected by subnet roaming issues.

Some companies, however, might want to implement multiple IP subnets across a common WLAN for various reasons, such as to make network management easier, facilitate location-based services, and decrease the spread of broadcast packets throughout the network. For instance, a company might want to deliver specific information to users based on their location in a specific building. By designating different subnets throughout the WLAN, the location of the user can be found and content delivered to the user based on their location. The location of the user in an airport, for example, could deliver a map of the applicable concourse or terminal, indicating flight information and the location of coffee shops and ticket counters. The system could also deliver advertisements from concessions located within the general area.

With multiple subnets mobile users must be able to seamlessly roam from one subnet to another while traversing a facility. As users roam across subnets, though, there must be a mechanism at Layer 3 to ensure that the user device configured with a specific IP address can continue communications with applications. Some controller-based WLAN implementations, such as Cisco using Layer 3 services, however, can solve this via a feature

called Proxy ARP, where a wireless client device can roam from an initial *anchor* controller to another *foreign* controller while maintaining the IP address originally assigned via the anchor controller. This is possible even though the foreign controller is operating on a different subnet than the anchor controller.

If the wireless solution you choose does not implement Proxy ARP, consider Mobile IP, which solves Layer 3 roaming by allowing the mobile user to use two IP addresses. One address, the home address, is static. The second address, the "care-of" address, changes at each new point of network attachment and can be thought of as the user's position-specific address.

The home address enables the mobile node to continually receive data relative to its home network, through the use of a network node called the home agent. Whenever the user is not attached to the home network, the home agent receives all the packets sent to the mobile user and arranges to deliver them to the mobile user's current point of attachment, which is its care-of address. Whenever a Mobile IP user moves, it registers its new care-of address with its home agent. This makes it possible for the home agent to keep up with the whereabouts of the mobile user. The home agent then sends any packets it receives for that user to the applicable care-of address.

To implement Mobile IP, you need two major components: a Mobile IP server and Mobile IP client software. The Mobile IP server will fully implement the Mobile IP home agent functionality, providing mobility management for the mobile users. The Mobile IP server can generally also keep track of where, when, and how long users use the roaming service. That data can then provide the basis for accounting and billing purposes.

The requirement for client-side software makes Mobile IP impractical for some applications. For example, public networks demand open connectivity for users, which makes it difficult to deploy solutions that require client software. Of course, the task of installing software on user devices before enabling roaming is too cumbersome. Another problem with Mobile IP is that it is somewhat vendor specific. To ensure interoperability among multivendor Mobile IP clients and servers, definitely do some upfront testing.

Wireless ISP Roaming

With Wi-Fi hotspots, there is very limited roaming among wireless ISPs. The Wi-Fi Alliance had tried developing standards several years ago to make wireless ISP roaming seamless, but the group later disbanded due to significant incompatibility among differing access controllers. In general, standards for roaming from one Wi-Fi wireless ISP to another are nonexistent. As a result, you must negotiate teaming agreements with other ISPs when deploying widespread Wi-Fi hotspots and create a custom access control system that is common among all applicable ISPs.

Wireless IP Phone Roaming

One the applications that roaming impacts a great deal are wireless telephony. If you plan to have wireless IP phones operating on the WLAN, ensure that the WLAN you design supports effective roaming. The voice user must be able to move about the facility, and

the system will need to allow roaming at both Layer 2 and Layer 3. Without smooth roaming, users will experience dropped calls.

Layer 2 roaming takes place when a wireless IP phone moves out of range of an access point and reassociates with a different access point. Because this type of roaming will occur frequently as users move about a facility, such as a warehouse or hospital, be certain that Layer 2 roaming is fast (ideally less than 100 milliseconds). This mid-call roam time is the amount of time that elapses after the last RTP packet is seen from the current access point and the first RTP packet seen from the access point that the wireless IP phone associates with.

When selecting wireless IP phones, be certain that they support fast roaming. The Cisco 7920 wireless IP phones, for instance, are specially designed to make Layer 2 roaming fast enough to avoid dropped calls. For example, a Cisco 7925 phone will initiate a reassociation process with a different access point if the phone does not receive three consecutive beacons from the existing access point and its unicast frame to the access point is not acknowledged. The 7920 also periodically scans for better access points and maintains a list of potential access points. A decision to roam is made on signal strength and signal quality metrics. The quality metric makes use of information provided by each access point in its beacon regarding the utilization of the access point. As a result, the phone can avoid attempting to reassociate with access points that have high utilization and may not be able to effectively support voice traffic. With these mechanisms, the 7925 is generally able to complete Layer 2 roaming within 100 milliseconds.

The addition of Layer 3 roaming might cause substantial delays that may drop voice calls. This will depend on the wireless solution that you implement, especially those that do not implement enhanced features for voice roaming. As a result, you might need to consider avoiding having wireless IP phones perform mid-call Layer 3 roaming. In this case, if possible, define a single subnet for the entire WLAN. This will completely avoid Layer 3 roaming. If this is not possible or feasible, at least minimize the possibility of Layer 3 mid-call roaming. For example, you may have a different subnet on each floor of a hospital. When performing the wireless site survey, ensure that signals from one floor do not overlap at such an extent that the wireless IP phones will roam to the floor above (or below) while the user is walking through a particular area.

Mobility Settings

Many WLAN product vendors enable you to indicate the degree of mobility of each station so that the access point can optimize roaming algorithms. If you set up the station as being “mobile,” the roaming protocols will enable the station to reassociate as it moves from one access point to another. If set to “mobile” mode, stationary devices, such as wireless desktops, might experience a short episode of radio signal interference and falsely reassociate with a different access point. As a result, stationary roaming modes usually take this into consideration.

Note Avoid the use of automatic/adaptive channel control on access points when implementing wireless IP phones. Frequently changing channels will cause the phones to roam frequently, which generally results in a higher and undesirable call drop rate.

Summary

It is important to pay close attention to aspects of the WLAN design that impact range, performance, and roaming. Bear in mind that sometimes range and performance indirectly proportional. As a result, have a good idea of whether range or performance is more essential before getting too far with the design. If focusing on maximizing range, consider signal coverage requirements, radio frequency bands, transmit power settings, transmission channel settings, data rate, antennas, amplifiers, repeaters, physical obstacles, and radio signal interference. If performance is important, consider radio frequency bands, transmit power settings, transmission channel settings, data rate settings, antennas, amplifiers, physical obstacles, radio signal interference, channel width settings, signal coverage, fragmentation settings, RTS/CTS settings, multicasting mechanisms, and microcell deployment strategies. To optimize roaming in cases where mobility is imperative, think about the various levels of roaming, special considerations for wireless IP phones, and mobility settings.

Index

2.4-GHz frequency band
interference tendencies of. *See* interference, RF
range of access for, 301
versus 5 GHz, 272-275
3G, WiMAX (802.16), 29
4G, WiMAX (802.16), 28, 29
5-GHz frequency band
capabilities of, 328
geographic legality issues, 272
increased performance of, 272
low interference benefit of, 273-274
range limitations of, 273
802 LAN standards family, 120-122
802.11 standards
802.11a, 21, 35
802.11b, 21-22, 35
802.11g, 22, 23, 35
802.11n, 23-24
benefits of, 117-120
Draft 2.0 of 802.11n standard, 23
features, list of, 129
initial 802.11, 20, 35
logical architecture of, 121-122
pre-802.11n issues, 23
table comparing, 24
target environments for, 129-130
url for, 129
802.11i security. *See also* WPA (Wi-Fi Protected Access)
802.1X port-based authentication, 151, 153
AES, basis for, 146-147
historic importance of, 35
TKIP (WEP2) basis of, 146
802.11k standard, 323
802.11r standard, 323
802.11s, 61
802.15 (Bluetooth), 30-32, 103-104
802.15.4 (ZigBee), 32-33
802.16. *See* WiMAX
802.1X port-based authentication
budgeting for, 221
EAP with, 342-344
mechanism of, 151, 153
802.2 LLC standard, 123. *See also* LLC (logical link control) layer

A

acceptance testing, 235
acceptance/verification testing, 406, 415-416
access network design
2.4-GHz *versus* 5 GHz, 272-275
ad hoc WLAN networks, 270-272
architectural considerations, 264
autonomous access point architecture, 265-266
controller-based access point architecture, 267-268
gateways, 270
lightweight access points, 267
mesh network architecture, 269-270
migration considerations, 276-277
primary architectures for, list of, 265
redundancy considerations, 277-281, 282
virtual WLANs, 274-276
access point (Layer 2) roaming, 322-323
access points
advantages over peer-to-peer transmissions, 58
antenna alignment, 395. *See also* antennas
autonomous, 68-69
autonomous access point architecture, 265-266
beacon interval configuration, 397-398
budgeting for, 220
certified, url listing, 69
channel width settings, 401
channels, configuring, 399-400. *See also* channels, RF
client radios, compatibility with, 443
collocated cells, 58
configuration of, 396-402
connecting. *See* network distribution systems
controller-based. *See* controller-based access points
disjointed cells, 58-59
DTIMs, 397
EIRPs of, 377-379
facility inspections to assess placement of, 372
failures of, 442
field upgrades, importance of, 68
firmware, updating, 350
identifying locations for, 384
installation, physical, 394-395
lightweight, with controllers, 267
maintenance of, 426, 428
mesh nodes compared to, 59-60
monitoring, 424
mounting above ceiling tiles, issues for, 394-395
optimizing locations for antennas, 379-385
passwords for, 350
physical security of, 395
PoE for, 79-82
power, signal, configuration of, 398-399
propagation testing, 379-383
redundancy issues, 279-281, 282
resetting, security issue with, 350
RF band configuration, 398
roaming, handling of, 110
rogue, 93-94, 346-347, 433-434
role in network architecture, 57-59, 68
routers, functionality added to, 70
safe distances from humans, 395
shutting down when unused, 350

spares, keeping, 428
SSID configuration, 396-397
troubleshooting configuration issues, 445-446
wireless site survey test units, 370, 371
accessing the medium. *See* medium access
ACK (Acknowledgment) frames
Duration field of, 173
error recovery role of, 140-141
spacing interval for, 156-158
acknowledged connectionless service, 128
Acme Healthcare case study
802.11n over legacy choice, 26
goals for WLAN upgrade, 15
Acme Industries case study
about Acme Industries, 203
access network architecture definition, 282
aesthetic requirements, 259
application connectivity, 297
application requirements, 241-243
budgeting, 224-225
client device requirements, 244
coverage requirements, 246
distribution system architecture, 284
environmental requirements, 256-258
existing infrastructure requirements, 255
integration requirements, 255-256
mobility requirements, defining, 250
project scope development, 206
purpose of, 201
requirements approvals, 260
risk evaluation planning, 226-227
scalability requirements, 254
scope of project, defining, 206
security requirements, defining, 253
staff identification for deployment, 217
utilization requirements, 248
VoWLAN architecture design, 289
WBS creation example, 213-214
WLAN deployment decision, 203
ACS (Access Control Server), Cisco, 344
action frames, 170-171
Active Frequency Hopping, Bluetooth, 103
active scanning, 149-151
ad hoc clients with access points, 443
ad hoc WLAN networks
architecture of, 270-272
beacon responsibility, 168
mechanics of, 55-57
adaptive mode, 332-333
Adaptive Wireless Path Protocol (AWPP), 61, 269
Address fields, MAC frames, 164-165
AES (Advanced Encryption Standard)
required for 802.11n encryption, 341
verifying configuration of, 413
WPA-2, basis for, 146-147
aesthetic requirements, 258-259
AIDC (automatic identification and data capture), 206
AirMagnet Laptop Analyzer, 110
AirMagnet Spectrum Analyzer
channel utilization, viewing, 375
noise floors, viewing, 374
AirMagnet Survey software, 304
AirPcap, 364
AirSnort, 432
ALOHANET, 34
alternative wireless technologies. *See* WiMAX

amplifiers, RF. *See* RF amplifiers
amplitude, radio wave. *See also* signal strength
attenuation of, 48-51
characteristics of, 41-40
inverse square rule, 49-50
modulation with, 43
QAM (quadrature amplitude modulation), 45
analysts, identifying for staffing, 215-217
Announce Protocol, 323
antennas
aesthetic requirements, 258-259
alignment during installation of access points, 395
bandwidth, 72
budgeting for, 220
characteristics of, 72-73
directional, 73-74, 380
diversity, 73
diversity configuration, 399-400
diversity, benefits of, 307
external, recommendation of, 66
gain, 73
high-gain, benefits of, 306
identifying locations for, 384
locations for, recommending, 385
misaligned, 446-447
optimizing locations for, 379-385
PC card, 67
performance issues, 315
placement tips, 394
power of, 72
propagation testing of, 307, 379-383
purpose of, 72
radiation patterns of, 72-74
range of access effects, 306-307
RF amplifiers with, 74-75
troubleshooting, 446-447
wireless site survey test units, 370
yagi, 73-74
application connectivity
Acme Industries case study, 297
architectural design considerations, 264
browser-based, 83, 292-293
databases, direct interfaces with, 84
distributed upgrades of applications, 294
programming environment limitations, 291
screen size issue, 291-292
site survey requirements reviews, 369
socket programming, 84
system architecture considerations, 289-297
terminal emulation, 82-83, 289-291
testing, 410
wireless middleware, 84-85, 294-297
applications
budgeting for software development, 221
connectivity. *See* application connectivity
software development, 210
testing, 410-411
approvals of requirements, 260
architecture, designing for a system. *See* system architecture design
architectures of networks
ad hoc networks, 55-57
infrastructure WLANs, 57-59
mesh networks, 59-62
types of, 55
ARP (Address Resolution Protocol) vulnerability, 92-93

ARQ (Automatic Repeat Request)
continuous ARQ, 126-127
design example, 128
go-back-n technique, 127
purpose of, 126
selective repeat technique, 127
stop-and-wait ARQ, 127-128
as-installed coverage testing, 407
AS/400 terminal emulation, 82
association
802.11g-only mode, 23
IDs for, 171
listen intervals, 171
MAC layer function for, 154-155
observing rate of, 142
performance testing of, 408-409
reassociation. *See* reassociation
request frames, 167
response frames, 167
service, 131
SSIDs for, 172
state of, 133
association frames
monitoring for coverage issues, 441
roaming, use in, 110
assumptions, stating for projects, 205-206
ATIM frames, 170
atmospheric conditions, 51
ATS (Automated Transport System) example, 6-9
attenuation
of signal strength, 48-51
RF shielding for security, 347-349
authentication
802.11 mechanisms for, 151-153
802.1X port-based, 151, 153, 342-344
authentication frames, 170
authentication state, 133
Cisco ACS (Access Control Server), 344
Cisco LEAP, 343, 410
deauthentication frames, 170
EAP (Extensible Authentication Protocol), 342-344
frames field variables for, 171
IAS (Internet Authentication Service), Microsoft, 344
open system authentication, 151-152
passwords, 443
RADIUS, 344
rogue access point prevention with, 94
server-based authentication, 151, 153, 342-344
servers, EAP-TLS based, 344
services defined by 802.11, 130
shared key authentication, 151-153
testing, 410
WEP issues, 410
X.509 for controller-based systems, 267
Automated Transport System (ATS) example, 6-9
autonomous access point architecture, 265-266
autonomous access points, 68-69
AWPP (Adaptive Wireless Path Protocol), 61, 269

B

backhaul link mesh network requirements, 270
backward compatibility requirements, 36. *See also* interoperability of 802.11 types

bands, frequency. ***See*** **frequency bands**
bandwidth control, performance enhancement from, 319-320
bandwidth, antennas, 72
bar code devices, 2-4, 20
batteries
beacon interval impact on, 169
limitations of, 110-111
beacon frames
ad hoc networks, in, 56-57
infrastructure WLANs, purpose in, 58
intervals, 168-169, 171
listen intervals, 171
observing, 170
passive scanning function of, 149
SSIDs (service set identifiers), 172
structure of, 168-169
timestamps, 168, 172
TIMs (Traffic Indication Maps), 171
beacons
frames. *See* beacon frames
interval configuration, 397-398
rates, signal coverage testing of, 407-408
testing for, 442
benefits of 802.11n over legacy WLANs
improved access to remote areas, 16-17
mobility improvements, 16
benefits of wireless networks
cost savings, 17
feasibility studies, including in, 228-229
installation in remote areas, 16-17
installation time, 17
mobility, 15-16
productivity, 18
qualitative benefits, 19
quantitative benefits, 19
reliability, 17
Block ACK Frames, 172
Block ACK frames, 140-141
Bluetooth
interference from, 103-104
standard, 30-32
bridges
budgeting for, 220
distance linkable by, 16
packet transmission by, 76
scenarios for using, 75-76
browser-based application connectivity
advantages of, 292
disadvantages of, 292-293
screen size issue, 83, 292
BSSIDs (basic service set IDs) Address fields, 164-165
BSSs (basic service sets), 57
budgeting for deployments
deployment services costs, 221-223, 224-225
design and requirements phase, 218-219
electricity costs, 223
equipment cost components, 219-221, 224
importance of, 218
installation budgets, 391
operations and maintenance costs, 223-225
spare hardware, 428
support costs, 223
buildings
floor plan diagrams for wireless site surveys, 371

floor plans requirements study, 256
physical obstacles to RF signals in, 50-51
requirements study of construction, 256

C

cables, Ethernet
budgeting for, 221
installing, 393-394
maximum effective length of, 78
call-processing agents, 287-288
CallManager, Cisco, 284-285, 287
capacity. *See also* data rates
determining, 321
increasing, 429
repeaters, reduction from, 308
CAPWAP (Control and Provisioning of Wireless Access Points), 267
CardBus, 66-67
carrier sense multiple access (CSMA), 97
carrier signals, 43
carrier-sense function, 179
CCBs (configuration-control boards), 430-431
ceiling tiles, mounting above, 394-395
cells, radio
collocated cells, 58
disjointed cells, 58-59
edge overlap recommendations, 338
overlap considerations, 383
overlapping separate, interference from, 105
roaming, overlapping required for, 58
role of, 57-58
utilization issues with, 447
cellular phones, VoWLAN replacement of, 5-11
certification, Wi-Fi, 24-25
certifications, values of employees with, 450-453
Certified Wireless USB, 33-34
CF (CompactFlash) radio cards, 67
CF End (contention-free end) frames, 173
change control, 430-431
change engineering, 428-430
channels, RF
adaptive mode, 332-333
bands of. *See* frequency bands
bonding, 193-194
choosing to avoid neighboring WLAN interference, 105-106
clear channel assessments, 179
configuring, 399-400
interference tests with, 100
manual channel settings, 328-332
multilevel facilities, settings recommendations for, 330-332
performance, effects on, 314, 446
range affected by, 303
single-level facilities, settings recommendations for, 329-330
troubleshooting, 443
width settings, 316-317, 401, 446
charters, project, 204-206
Cisco ACS (Access Control Server), 344
Cisco certifications, 452-453
Cisco Discovery Protocol PoE device detection, 79
Cisco LEAP (Lightweight Extensible Authentication Protocol), 343, 410

citywide WiFi deployments
indoors, issues for coverage, 311
mounting assets, evaluation of, 385-386
planning for, 235
signal indoor coverage testing, 408
clear channel assessments, 179
client devices
budgeting for, 219
firmware, updating, 350
power-saving mode, effect on throughput, 313
radios of. *See* client radios
registration testing, 409-410
requirements determination for, 243-244
requirements impact on site surveys, 369
selection criteria, 62-63
signal strength issues, 441
unauthorized, testing, 414
uplink signal strength, 377-379
wipe functions for, 63
client radios
ARP (Address Resolution Protocol) vulnerability, 92-93
budgeting for, 219
CardBus, 66-67
certified, url listing, 69
CompactFlash (CF) form factor, 67
configuration settings, 443
ExpressCard standard, 67
incompatibility issues, 442
interface form factors, 65-68
ISA bus with, 66
Mini-PCI cards, 66
multimode, 64
PC cards, 66-67
PCI bus with, 66
power to performance relationship, 313
receiver sensitivity values, 376
software drivers, 64
specifications for, 63-68
transmit power settings, 443
troubleshooting, 443, 445
uplink signal strength, 377-379
USB (Universal Serial Bus) based, 67-68
client/server systems
application architecture issues, 291
middleware, advantages for, 296
collocated cells, 58
communications rooms, 372
CompactFlash (CF) radio cards, 67
compatibility. *See also* interoperability of 802.11 types
802.11 standards comparison, 24
802.11n requirements for, 36
compression capabilities of wireless middleware, 295
configuration
access points settings, 396-402
antenna diversity, 399-400
beacon intervals, 397-398
change control of, 430-431
channel width settings, 401
client radio settings, 443
data rates, 399
definition phase for components, 208
documentation of, 403
DTIMs, 397
enabling 802.11n, 396-397
fragmentation thresholds, 401-402
implementation phase for components, 210

monitoring, 425
radio frequency bands, 398
RTS/CTS (request-to-send/clear-to-send), 402
signal power, 398-399
SSIDs, 396-397
verifying, as a security policy, 433
configuration-control boards (CCBs), 430-431
connection-oriented service, 125-126
connectivity
as MAC layer function, 136
association step, 154-155. *See also* association
authentication mechanisms, 151-153
coverage, insufficient, 441
exercise for observing, 155
help desk responses to problems with, 422
MAC layer function, components of, 136
scanning for networks, 149-151
steps required to make connections, 148-149
testing, 409-410
troubleshooting, 440-443
constraints, stating for projects, 205-206
contention
CF End (contention-free end) frames, 173
DCF protocol for, 138-139
continuous ARQ, 126-127
continuous movement, 248
control frames, 132-133, 172-173
Control Wrapper frames, 172
controller-based access points
architecture for, 267-268
controllers for. *See* controllers
lightweight nature of, 69-70
LWAPP (Lightweight Access Point Protocol), 267
controllers
beacon interval configuration, 397-398
budgeting for, 220
configuring channels, 399-400
determining number needed, 268
enabling 802.11n, 396-397
features provided by, 267
Proxy ARP for roaming, 324
redundancy issues, 277
SSID configuration, 396-397
transmit power configuration by, 398-399
converting power units, 53
cordless phone-based interference, 101-102
costs
budgeting. *See* budgeting for deployments
electricity costs, 223
enterprise wireless *versus* wired, 13
identification for deployments, 228
reorganizations, resulting from, 17
standards, impact of, 119
coverage
acceptable, definition of, 376
antenna diversity to improve, 73
difficult to cover and unusual areas, 245, 333-337
elevators, 245, 333-335
expanding to new areas, 429
heat maps, 358-361
hospital environment example, 5, 8
insufficient, troubleshooting, 441
interference affecting. *See* interference, RF

keeping within a facility for security, 350-351
maintenance issues, 426-427
minimum received signal strength, 376
parking areas, 336-337
performance effects of, 317, 444
problems, help desk responses to, 423
requirements for, determining, 244-246
requirements impact on site surveys, 369
signal coverage testers, 358-362
SNR minimums, 376
stairwells, 245, 336
surveying. *See* wireless site surveys
uplink signal values required for, 377-379

CPE (customer premises equipment), 311

CSMA (carrier sense multiple access)
DCF implementation of, 138-139
jamming with, 97

CTS (clear-to-send) frames
CTS-to-self mechanism, 174-175
spacing interval for, 156-157
TRS frames, relation to, 173

customer premises equipment (CPE), 311

CWNP (Certified Wireless Network Professional) program, 452-453

D

DAs (destination addresses), 165

data bundling, 296

data delivery function, MAC layer
components of, 136
data frame fragmentation, 143-144
data frames for, 136-137
encryption function, 145-147. *See also* encryption
error recovery, 140-142
frame aggregation, 142-143
HCF (hybrid coordination function), 139-140
medium access, 137-140
MPDUs, 137
MSDUs, 137
multicasting, 147-148

data frames
ACK and Block ACK, 140-141
aggregation of, 142-143
dynamic rate switching, 141-142
fragmentation in, 143-144. *See also* fragmentation
maximum size of, 136
MSDUs *versus* MPDUs, 137
null, 174
payloads of, 174

data link layer, OSI model, 121-122. *See also* MAC layer

data rates
auto setting recommended, 304
configuration, 399
distance to access points, relation to, 300
dynamic rate switching, 141-142
Ethernet, required to support 802.11n, 78
performance, effects of settings on, 315, 445
range of access effects from, 304-305
receiver sensitivity values, variance with, 376
relation to cell range, 58
supported rates field, 172
throughput *versus,* 312-313

databases, direct wireless interfaces with. ***See*** **direct database connectivity**
dBm units, 40, 53
DCF (distributed coordination function), 137, 138-139
DCF IFS, 157
deauthentication service, 131
demodulation, PMD sublayer role in, 178
denial-of-service (DoS) attacks, 95-96
deployments. ***See also*** **installation**
acceptance testing, 235
application software development for, 210
budgeting for. *See* budgeting for deployments
citywide WiFi deployments, 235
deciding whether to proceed, 229-232
evaluating, 233-234
implementation phase planning, 209-211
kick-off meetings, 232
managing, 232-233
operations phase of deployments, 211-212
planning for. *See* planning for deployments
procurement issues, 209-210
progress reports, 233
project execution, 232-233
status checks, 233
technical interchange meetings, 233
design phase of deployment projects
Acme Industries example, 213-214
components of, 207-209
design reviews for system updates, 430
desktop support groups, 436
destination addresses (DAs), 165
detection of signals. ***See*** **carrier-sense function**
DHCP (Dynamic Host Configuration Protocol)
dedicated servers recommended for larger networks, 71
subnet roaming issues, 323
Wi-Fi router provision of, 70-71
DIFS (DCF IFS), 157
direct database connectivity
advantages of, 293-294
disadvantages of, 294
distributed upgrades of applications, 294
wireless interfaces with, 84
direct-sequence spread-spectrum. ***See*** **DSSS (direct-sequence spread-spectrum)**
directional antennas, 73-74
disassociation
deauthentication with, 131
frame attacks, 95
frames, 170
frames, use in roaming, 110
service for, 131
disjointed cells, 58-59
distance, effect on signal strength, 49-50
distributed coordination function (DCF), 137-139
distribution system services
association service, 131
disassociation service, 131
integration service, 132
purpose of, 131
reassociation service, 132

distribution systems
architectural design considerations, 264
PoE architecture, 282-283
switches, 282
diversity, antenna, 73
doctor offices. *See* healthcare industry
documentation
designs for projects, 208
installations, 211, 403
requirements for projects, 207, 259-260
wireless site survey report generation, 385
DoS (denial-of-service) attacks, 95-96
Draft 2.0 of 802.11n standard
certifications based on, 37
device compatibility issues with, 111
upgrading prior products to, 23
Draft 3.0 of 802.11n standard, 37
DSSS (direct-sequence spread-spectrum)
802.11, initial, 20
802.11b, 22
example of modulation with, 46
HR-DSSS (802.11b), 188-190
physical layer legacy, 182-185
DTIMs (delivery traffic indication messages), 147-148, 397
durability requirements study, 257
Duration fields
MAC frame Duration/ID field, 164
medium access use of, 139
of ACK frames, 173
duty cycles, 356
Dynamic Host Configuration Protocol. *See* DHCP
dynamic rate switching, 141-142

E

EAP (Extensible Authentication Protocol), 153, 342-344
EAP-TLS (Extensible Authentication Protocol-Transport Layer Security), 344
effective isotropic radiated power (EIRP), 377-379
EIFS (Extended IFS), 157-158
EIRP (effective isotropic radiated power), 377-379
Ekahau Site Survey software, 304
electromagnetic waves. *See* radio waves
elevators, coverage issues, 245, 333-335
employees. *See* staffing
encryption
AES (Advanced Encryption Standard), 146-147, 341, 413
common key concept, 340
IPsec, 349
Layer 2 *versus* Layer 3, 341
methods for, overview of, 145
passive monitoring exercise with, 90
passive monitoring, as countermeasure to, 88
public key encryption, 342
recommended as a policy, 349
SSL, 90
TKIP, 146
types available, list of, 341
WEP2, 146
WPA *versus* WEP, 349
engineering for operational support, 428-430

engineers
identifying for deployment projects, 215-217
network engineering staff, 450
environmental requirements, 256-258, 370
equipment
certified Wi-Fi list url, 24
client. *See* client devices
wireless access points. *See* access points
ERP (Extended-Rate PHY 802.11g), 190
error control
connection-oriented service for, 125-126
FEC (forward error correction), 126
error recovery
ACK (Acknowledgment) frames, 140-141
Block ACK frames, 140-141
dynamic rate switching, 141-142
purpose of, 140
ESS (extended service sets), 58. *See also* infrastructure WLANs
Ethernet
data rates required to support 802.11n, 78
existing infrastructure requirements, 254
power over. *See* PoE (Power over Ethernet)
switches. *See* switches, Ethernet
evaluating deployments, 233-234
existing infrastructure
assessing for wireless site surveys, 372-373
communications rooms, 372
power over Ethernet. *See* PoE (Power over Ethernet)
reporting on, 385
requirements, 254-255
switches, *See* switches, Ethernet
WAN capability, existing, 373
ExpressCard standard, 67
Extended IFS, 157-158
extended service sets (ESS), 58
Extended-Rate PHY (ERP) 802.11g, 190

F

facilities
changes required for installation, 390
inspections of, 372
Faraday cages, 347
Fast Fourier Transforms (FFTs), 354-356
feasibility studies
Acme Industries case study, 231-232
benefits, 228-229, 231
costs, 228, 231
deciding whether to proceed, 229-232
impacts on existing systems, 229-232
impacts on users, 229-231
key factors for, 227-228
features of 802.11 standard, list of, 129
FEC (forward error correction), 126
FFTs (Fast Fourier Transforms), 354-356
FHSS (Frequency-Hopping Spread-Spectrum)
Bluetooth, for, 31, 103
interference issues, 106
interoperability issues, 112
legacy physical layer specification, 180-182

firmware
performance effects of, 445
troubleshooting, 442
updating, 350, 427-429
floor plans
diagrams for wireless site surveys, 371
requirements study, 256
flow control, connection-oriented service for, 125-126
FMC Technologies, Inc., 6-9
fragmentation
fragments, numbering in frames, 165
retransmissions from insufficient, 318
settings, performance effects of, 317-318
thresholds, configuring, 401-402
troubleshooting, 446
Frame Check Sequence field, 166
frames
ACK and Block ACK, 140-141
aggregation, 142-143
data frame fragmentation, 143-144
Duration fields, 139
More field, 144
observing typical, 175
purpose of, 137
spacing intervals. *See* IFS (interframe space) intervals
station states, types allowed with, 132-133
traces of, recording, 363
viewing with protocol analyzers, 362-365
free space loss (FSL), 49-50
FreeRADIUS, 344
frequency bands
2.4 or 5-GHz, selecting between, 327-328
39. *See* 2.4-GHz frequency band
5-GHz. *See* 5-GHz frequency band
channels in. *See* channels, RF
configuration of, 398
frequency hopping, 46-48
frequency, RF
802.11 bands40. *See also* frequency bands
FSK (frequency shift-keying), 43-44
waves, as attribute of, 41-40
From DS field, MAC frames, 161
FSK (frequency shift-keying), 43-44
FSL (free space loss), 49-50

G

G.711 codecs, 284
gain, antenna, 73, 306
gatekeepers, H.323, 287
GFSK modulation (FHSS legacy), 182
guest access, 345

H

Handover Protocol, 323
Hayes, Vic, 35
HC Control field, 166
HCCA (HCF controlled channel access), 139-140
HCF (hybrid coordination function), 137-140
healthcare industry
802.11n over legacy choice26
Acme example. *See* Acme Healthcare case study

applications of WLANs for, 4-5
hospital wireless site surveys, 380-381
locations-based services, 14
Ohio State University Medical Center example, 6-9
USC University Hospital VoWLAN case study, 11
WLAN effects on medical devices, 99
heat maps, 304-361
help desks
experience requirements for staffing, 450
responsibilities of, 422-423
trouble tickets, handling, 435-436
hidden nodes issues, 158-159
history of WLANs
802.11a, 35
802.11b, 35
802.11g, 35
802.11n standardization, 36-37
initial 802.11 standardization, 35-36
pre-802.11 networks, 34-35
home WLANs, 12
hospitality industry WLAN use, 5
hospitals. *See* healthcare industry
HR-DSSS (802.11b), 188-190
HT-OFDM
channel bonding, 193-194
mixed mode operation, 198
modulation, 194-195
multiple-input multiple-output. *See* MIMO
HTSG (High Throughput Study Group), 36
hubs, Ethernet, 77-79
human factors in deployments, 229
humidity requirements study, 256-257
hybrid coordination function (HCF), 137, 139-140

I–J

IAPP (Inter-Access Point Protocol), 322-323
IAS (Internet Authentication Service), Microsoft, 344
IBSSs (independent basic service sets), 56
IEEE (Institute for Electrical and Electronic Engineers), 117
IEEE 802 LAN standards family, 120-122
IEEE 802.11 Working Group, 18
IEEE 802.11. *See* 802.11 standards
IEEE 802.15 (Bluetooth), 30-32
IEEE 802.15.4 (ZigBee), 32-33
IEEE 802.16 Working Group, 18
IEEE 802.16. *See* WiMAX
IEEE 802.2 LLC standard, 123. *See also* LLC (logical link control) layer
IFS (interframe space) intervals
DCF IFS, 157
Extended IFS, 157-158
PCF IFS, 157
short IFS, 156-157
implementation phase of deployments
evaluating, 233-234
implementers, identifying, 215-217
kick-off meetings, 232
planning, 209-213
progress reports, 233
status checks, 233
technical interchange meetings, 233
in-motion testing, 406, 412-413. *See also* roaming

incompatibility issues between client radios and 802.11n access points, 442
independent basic service sets (IBSSs), 56
infrared physical layer, 185
infrastructure components
application connectivity software, 82-85
hubs, Ethernet, 77-79
network distribution systems, 77-79
optical fiber, 79
PoE. *See* PoE (Power over Ethernet)
switches, Ethernet, 77-79
terminal emulation, 82-83
types of, 77
wireless middleware, 84-85
infrastructure WLANs
architecture of, 57-59
collocated cells, 58
data flows, typical, 58-60
disjointed cells, 58-59
roaming requirements, 58
initial 802.11, 20, 35
installation
access point physical installation, 394-395
autonomous access points disadvantages for, 266
benefits of wireless over wired, 16-17
budgets for, 391
cabling, laying, 393-394
configuring access points, 396-402
considerations for, 211
control policy for, 425
coordinating with management and employees, 391-392
documentation of, 403
documentation prior to, 390
facility changes, planning, 390
major components to plan for, 388
managers of, 388
mounting access points, 394-395
plans, developing, 388-391
points of contact, 388-389
preinstallation meetings recommended, 392
procedures for, planning, 389-390
resource identification, 391
risk assessments, 391
safety tips for, 389
scheduling, 390-391
staging components, 392-393
steps for, 387
switches, 393-394
tests to perform after, 402
tools for, 390
wireless surveys, necessity of, 112-113
Institute for Electrical and Electronic Engineers. *See* IEEE
integration requirements, 255-256
integration service, 132
Inter-Access Point Protocol (IAPP), 322-323
interference, RF. *See also* noise
5 GHz band low interference benefit, 273-274
802.11 protocol, effects on, 97-98
802.11 standards comparison, 24
Bluetooth-based, 103-104
cataloging possible sources of, 358
channels, changing to avoid, 303, 329-330
cordless phone-based, 101-102
denial-of-service attacks, 95-96
duty cycles, 356
effects of, 97-98
FHSS-based, 106

microwave-oven based, 21, 22, 99-100
neighboring WLANs, from, 105-106
performance effects of, 316-317, 444
range of access effects of, 309-310
reducing, tips for, 337
RF shielding against, 348
signal-to-noise ratio, 51-53, 54
SNR (signal-to-noise ratio), effects on, 98. *See also* SNR (signal-to-noise ratio)
swept spectrograms, 357
testing, steps for, 107
troubleshooting, 442-444
Wi-Fi with ZigBee, 33
wireless site survey identification of, 373-375
WLAN effects on medical devices, 99

interoperability of 802.11 types
802.11 standards comparison, 24
802.11n mixed-mode, 198
802.11n requirements for, 36
CTS-to-self mechanism, 174-175
issues affecting, 111-112
vendor-specific device issues, 118-120

interviewing staff for requirements determinations, 239-240

IP addresses
Mobile IP, 324
required at access points for CAPWAP, 267
sharing Wi-Fi routers for, 70-71
subnet roaming issues, 323-324

IP domains, creating separate for WLANs, 79

IP phone roaming, 324-325. *See also* roaming; VoWLAN (Voice over WLAN)

IPsec
multiple concurrent session support, 72
VPNs based on, 349

ISA (Industry Standard Architecture) bus, 66

ISM (Industrial, Scientific, and Medical) bands, 35

ISO 8802-nnn, 120

ISP roaming, 324

K–L

key requirements of 802.11n, 36

keys, encryption, 342

kick-off meetings, 232

Lamarr, Hedy, 48

latency
interference-based, 97
mesh networks, issues with, 61

Layer 1, OSI model, 121-122

Layer 2
encryption, 341
OSI model, 121-122
roaming, 322-325

Layer 3
encryption, 341
roaming, 323-325

LBSs (location-based systems). *See* location-aware services

LEAP (Lightweight Extensible Authentication Protocol), 343, 410

legacy 802.11 systems
DSSS physical layer, 182-185
ERP (Extended-Rate PHY) 802.11g, 190
FHSS physical layer, 180-182
HR-DSSS (802.11b) physical layer, 188-190

infrared, 185
OFDM physical layer, 185-188
physical layers of, 180-190
protection mechanisms in 802.11n for interoperability, 174-175
legacy 802.11 systems. *See* 802.11 standards
Lightweight Access Point Protocol (LWAPP), 267
lightweight access points, 267
LLC (logical link control) layer
acknowledged connectionless service, 128
ARQ (Automatic Repeat Request), 126
connection-oriented service, 125-126
continuous ARQ, 126-127
Control field, 124
Data field, 124
DSAP field, 124
FEC (forward error correction), 126
PDU format of, 124
relation to other layers, 121-123
services provided by, 123-124
specification of, 123
SSAP field, 124
stop-and-wait ARQ, 127-128
unacknowledged connectionless service, 124-125
load testing, 411
locating access point antennas, 379-385
location-aware services
applications for, 13-15
case study of, 15
locations of equipment, documenting, 403
LWAPP (Lightweight Access Point Protocol), 267

M

MAC addresses
broadcast addresses, 147
client radio use of, 92-93
fields for, 164-165
types of, 165
MAC frames
Address fields, 164-165
Duration fields, 139
Duration/ID field, 164
format, overall, 160-161
Frame Body field, 166
Frame Check Sequence field, 166
From DS field, 161
HC Control field, 166
management frames, 167-172
More Data field, 164
More Frag field, 161-163
Order field, 164
power management field, 163
Protected Frame field, 164
protocol version field, 160
QoS Control field, 166
Retry field, 163
Sequence Control field, 165
Subtype field, 161-163
To DS field, 161
Type field, 161
types of, 166-174
MAC frames. *See* also MPDUs (MAC protocol data units)
MAC layer
association mechanism, 154-155
client radio implementation of, 64
connectivity function. *See* connectivity
data delivery function, 136

data frame aggregation, 142-143
data frame fragmentation, 143-144
DCF (distributed coordination function), 137-139
dynamic rate switching, 141-142
encryption function, 145-147. *See also* encryption
error control, 122
error recovery, 140-142
frames of. *See* MAC frames
functions of, list of main, 136
interference issues, 106
medium access, 137-140
MPDUs, 137
MSDUs (MAC service data units), 129, 137
multicasting, 147-148
OSI model equivalent, 121-122
peer-to-peer issues, 56
physical layer communication, 178
power management function, 159-160
purpose of, 121-122, 135-136
timing and synchronization, 136, 156-158
transmission collisions, 123

maintenance
access points, of, 426-428
broken hardware issues, 427
change engineering, 428-430
experience requirements for staffing, 450
firmware updates, 427
performance issues, 426
planning for, 211-212
signal coverage issues, 426-427
spare hardware for, 428
staff for, identifying, 215-217
training staff for, 416

man-in-the-middle attacks, 92

management frames
action frames, 170-171
association request frames, 167
association response frames, 167
ATIM frames, 170
authentication frames, 170
beacon frames, 168-171
body elements of, 171-172
capability information, 172
deauthentication frames, 170
disassociation frames, 170
Duration field of, 167
functions available in, 132-133
probe request frames, 168
probe response frames, 168
purpose of, 167
reassociation request frames, 167
reassociation response frames, 167
SSIDs (service set identifiers), 172
status codes, 171
supported rates field, 172

management of WLANs. *See also* operational support
autonomous access points disadvantages for, 266
security management, 431-434

managers
implementation managers, 215-217
installation managers, 388
project managers, 215-217

managing deployments, 232-233

medical uses of WLANs. *See* healthcare industry

medium access
DCF (distributed coordination function), 137, 138-139
HCCA, 139-140
HCF (hybrid coordination function), 137-140

NAVs (network allocation vectors), 139
PCF (point coordination function), 137
random back offs, 139
mesh networks
802.11s standard for, 61
advantages of, 60
ADWPP (Adaptive Wireless Path Protocol), 269
architecture of, 59-62, 269-270
citywide hot zones, 62
extending from outdoors to indoors, 311
gateways to, 270
latency issues, 61
nodes of. *See* mesh nodes
performance issues, 270
mesh nodes
capabilities of, 72
multi-radio, benefits of, 72
powering, 62
routing protocols of, 61
metal obstructions, 394
MGCP (Media Gateway Control Protocol) for PSTN, 285
microcell deployment strategies, 319-320
microwave-oven based interference, 21-22, 99-100, 358
middleware. *See* wireless middleware
migration
considerations for, 276-277
terminal emulation client/server support lacking, 291
to future systems, 119
MIMO (multiple-input multiple-output)
advantages of, 23, 190
spatial multiplexing, 191-193
transmit beamforming, 190-191
Mini-PCI cards, 66
mixed mode operation
802.11n issues, 198
b/g mixed mode issues, 22-23
testing for, 411
Mobile IP, 324
mobility. *See also* roaming
in-motion testing, 406, 412-413
requirements impact on site surveys, 369
requirements, defining, 248-250
settings for, 325-326
modulation
amplitude key-shifting, 43
carrier signals, 43
FSK (frequency shift-keying), 43-44
HT-OFDM (802.11n), 194-195
mechanics of, 42-45
OFDM, 48
PMD sublayer role in, 178
PSK (phase shift-keying), 45
QAM (quadrature amplitude modulation), 45
source data signals, 43
spread spectrum, 45-48
monitoring wireless networks
access point monitoring, 424
configuration monitoring, 425
performance monitoring, 424
periodic testing policy, 426
security policy management, 425-426
More Data field, 164
More field, 144
More Frag field, 161-163
mounting access points, 394-395
mounting asset assessment, 235
MPDUs (MAC protocol data units)
components of, 137
Duration frames, 139
frame aggregation, 143

MSDUs (MAC service data units)
data frames carrying, 174
delivery of, centrality to 802.11, 129
delivery, frame types for, 166-174
fragments, numbering in frames, 165
frame aggregation, 143
More Frag field, 161-163
relationship to frames, 137
multicasting, specifications for, 147-148
multilevel facilities, channel recommendations for, 330-332
multimode radios, 64
multipath propagation
error detection and performance degradation, 108-109
mechanics of, 51
multisite WAN with centralized processing architecture for VoWLAN, 285-287
multisite WAN with distributed call processing for VoWLAN, 287-288
municipal deployments. *See* citywide WiFi deployments
mWs (milliwatts), 40

N

NAT (Network Address Translation), 70-71
NAVs (network allocation vectors), 139, 173
NetStumbler, 354, 361-362
Network Address Translation (NAT), 70-71
network allocation vectors (NAVs), 139, 173
network distribution systems. *See also* infrastructure components
cables, maximum effective length of, 78
hubs, Ethernet, 77-79
IP domains for, 79
lack of 802.11 standard for, 77
optical fiber infrastructure, 79
switches, Ethernet, 77-79
network engineering staff, 450
network support groups, 436
NICs (network interface cards), wireless, 65. *See also* client radios
nodes
hidden, RTS/CTS for, 158-159
mesh, 269
noise
duty cycles, 356
error control with connection-oriented service, 125-126
floors of, identifying, 373-375
signal-to-noise ratio, 51-54
null data frames, 174
nuttcp, 107

O

ODBC (Open Database Connectivity), 84
OFDM (orthogonal frequency-division multiplexing)
802.11a use of, 21
802.11g use of, 22
advantages of, 48
channel frequencies of, 187
data rates with modulation techniques, table of, 187-188
HT (802.11n). *See* HT-OFDM
PLCP frame fields of, 186
PPDUs of, 185
official standards, 115-116
Ohio State University Medical Center (OSUMC), 6-9

omnidirectional antennas, 73-74
open system authentication, 151-152
operational support
change control, 430-431
configuration management, 430
desktop support groups, 436
elements of, 421-422
engineering, 428-430
help desks, 422-423, 435-436
maintenance issues, 426-428
monitoring networks, 424
network support groups, 436
security management, 431-434
staffing for. *See* operational support staffing
transferring to operational mode, 436-437
trouble ticket systems, 435-436
operational support staffing
availability of existing staff for, 450
certifications, values of employees with, 452-453
education requirements, 451-452
experience requirements, 450-451
help desk experience requirements, 450
maintenance experience requirements, 450
qualifications for candidates for, 449-450
sources for potential employees, 453
training requirements, 451-452
operations phase of deployments
planning, 211-212
power costs, 223
staff for, identifying, 215-217
support costs, 223
training staff for, 416
OPNET simulation program, 321
optical fiber infrastructure, 79
Order field, MAC frames, 164
orthogonal frequency-division multiplexing. *See* OFDM
OSI (Open Systems Interconnection) model, 121-122
OSUMC (Ohio State University Medical Center), 6-9
other-than 802.11 wireless technologies. *See* WiMAX (802.16)
outdoor areas
access point requirements, 395
coverage issues, 245, 257
overlapping cells, 105, 383

P

packet sniffers
in-motion testing with, 412
security mechanism verification with, 413
wireless security vulnerability to, 88-91
parking area coverage, 336-337
PARs (Project Authorization Requests), IEEE, 117
passive monitoring vulnerability, 88-91
passive scanning, 149-150
passwords
connection failures from wrong, 443
for access points, 350
patient records. *See* healthcare industry
payloads, data, 166
PC cards, 66-67
PCF IFS, 157
PCI (Peripheral Component Interconnect) bus, 66
peer-to-peer WLAN architecture, 55-57

penetration testing
performing regular, 434
periodic testing, 426
types of testing, 414-415
performance
acceptable signal strength values, defining, 376-379
amplifiers for increasing, 316
antenna issues, 315
antennas, troubleshooting, 446-447
association testing, 408-409
bandwidth control for, 319-320
channel settings effects, 314, 446
channel width settings, 316-317
coverage requirement, 317, 444
data rate settings effects on, 315, 445
elements contributing to, list of, 311-312
firmware, effects of, 445
fragmentation settings, 317-318
interference, effects of, 316-317, 444
load testing, 411
maintaining, 426
mesh network issues, 270
microcell deployment strategies for, 319-320
monitoring, 424
problems, help desk responses to, 423
range, *versus*, 299-300
registration testing, 409-410
RF band choice effects on, 313
RTS/CTS effects, 318-319, 446
testing, 406
testing with interference, 107
throughput *versus* data rates, 312-313
transmit power settings, 313
troubleshooting problems with, 444-447
utilization requirements, 246-247
pharmaceutical tracking applications, 5
phase, wave
PSK (phase shift-keying), 45
QAM (quadrature amplitude modulation), 45
relation to other wave elements, 41
phones, WLAN. *See* VoWLAN (Voice over WLAN)
PHY (physical) layer
architecture of, 177-179
carrier-sense function of, 179
channel bonding, 193-194
client radio implementation of, 64
DCF use of, 138
DSSS legacy physical layer, 182-185
ERP (Extended-Rate PHY 802.11g) legacy, 190
FHSS legacy specification, 180-182
functions overview, 179-180
HR-DSSS (802.11b) legacy, 188-190
infrared, legacy, 185
legacy physical layers, 180-190
MAC layer communication, 178
OFDM legacy layer, 185-188
physical layer, OSI model, 121-122
PLCP sublayer, 177-178
PMD sublayer, 178-179
PSDUs (PLCP service data units), 178
receive function of, 180
spatial multiplexing, 191-193
specifications of, 123
transmit beamforming, 190-191
transmit function of, 179
physical addresses. *See* MAC addresses
physical layer, OSI model, 121-122. *See also* PHY layer

physical obstacles
attenuation due to, 50-51
range of access effects from, 309
physical security
location-based systems for, 14
of access points, 350, 395
switch and controller placement, 393
PIFS (PCF IFS), 157
pilot testing, 406, 418
planning for deployments
Acme Industries. *See* Acme Industries case study
application software development, 210
assumptions, stating, 205-206
budgeting. *See* budgeting for deployments
charters, project, 204-206
component configuration definition, 208
constraints, stating for projects, 205-206
deciding whether to proceed, 229-232
design verification, 208
experience level of staff, issues with, 226
feasibility analysis. *See* feasibility studies
geographical issues, 226
goals of, 203
human factors in deployments, 229
implementation phase planning, 209-211
importance of, 201
installation, considerations for, 211
operations phase of deployments, 211-212
pilot sites, 210
procurement issues, 209-210
product selection, 208
project management principles, 202-203
requirements, defining, 206-207, 226, 235
risk evaluation, 225-227
scheduling, 217, 226
scope of project, defining, 204-206
staffing, identifying, 214-217
steps for, 204
verification testing, 211
work breakdown structure creation, 206-214
PLCP (physical layer convergence procedure) sublayer
architecture of, 177-178
carrier-sense function, 179
receive function of, 180
transmit function of, 179
PMD (physical medium dependent) sublayer
architecture of, 178-179
carrier-sense function, 179
transmit function of, 179
PoE (Power over Ethernet)
advantages for wireless networks, 79-82
assessing existing for wireless site surveys, 373
budgeting for, 220
enhanced, 283, 373
network design considerations, 282-283
points of contact for installations, 388-389
polling by HCCA, 139-140
port scanners, 414-415
portable access requirements, 249
power management
beacon interval impact on batteries, 169

cost of operations, 223
deployment issues, 110-111
MAC layer role in, 136
multicasting effects on clients, 148
outage considerations, 283
power management field, MAC frames, 163
power-saving mode, effect on throughput, 313
PSMP, 160
SMPS, 159-160
Power over Ethernet. *See* PoE
power save multi-poll (PSMP), 160
power, signal. *See also* signal strength
adjusting for devices, 40
amplitudes of radio waves, 41-40
antennas, 72
attenuation of, 48-51
client radio transmit power settings, 443
configuration of, 398-399
converting dBm to mW units, 53
EIRP (effective isotropic radiated power), 377-379
performance, effect on, 313, 316, 445
range of access dependence on, 302-303
PPDUs (PLCP protocol data units)
FHSS legacy fields, 180-181
mixed mode fields, 198
purpose of, 178
pre-802.11n issues, 23, 36, 111
printing
bar codes. *See* bar code devices
home Wi-Fi print servers, 12
security concerns with, 95
security issues for, 414
privacy service, 131. *See also* encryption
probe requests
active scanning with, 150-151
frames for, 168
SSIDs (service set identifiers), 172
probe responses, 168, 172
process control applications, 128
procurement issues, 209-210
productivity benefits of wireless networks, 18
project charters, 204, 206
project management, 202-203
project managers, identifying, 215, 217
propagation of signals
attenuation of, 48-51, 347-349
multipath propagation, 51, 108-109
physical obstacles to, 50-51
propagation testing, 379-383
proprietary enhancements to 802.11, interoperability issues, 112
proprietary wireless standards, 116
Protected Frame field, 164
protocol analyzers
active scanning test with, 151
connection steps, following, 155
observing typical frames, 175
recording traces with, 362-363
WireShark, 364-365
protocol version field, MAC frames, 160
prototype testing, 406, 417-418
Proxy ARP, 324
PS (power-save) Poll frames, 173
PSDUs (PLCP service data units), 178-180
PSK (phase shift-keying), 45
PSMP (power save multi-poll), 160

public key encryption, 342
public networks, security issues, 414-415
public service applications, location-based systems for, 14
public standards, 115-116

Q

QAM (quadrature amplitude modulation), 45
QoS (Quality of Service)
HC Control field, 166
multicasting effect on, 147
QoS Control field, MAC frames, 166

R

radiation patterns of antennas, 72-74
radio signal interference. *See* interference, RF
radio waves
amplitude of, 41-40
attenuation of, 48-51
attributes of, 39-41
carrier signals, 43
frequency of, 40-41
FSL (free space loss), 49-50
multipath propagation, 51
nature of, 39
phase of, 41
physical obstacles, attenuation due to, 50-51
power, measurement of, 40-41
propagation of, 40
radios frequency amplifiers. *See* RF amplifiers
radios frequency systems. *See* RF systems
radios, client. *See* client radios
RADIUS, 344
rain, 51
random back offs, 139
range of access. *See also* coverage
amplifiers for increasing, 307-308
antenna effects on, 306-307
approximating for a particular site, 384
data rate setting effects, 304-305
interference effects on, 309-310
performance, *versus*, 299-300
physical objects, effects of, 309
relation to data rate, 58
repeaters, benefits from, 308
RF bands, differences for, 301
signal coverage requirements for, 300-301
signal-to-noise effects on RF bands, 301
transmission channel settings, 303
transmit power, dependence on, 302-303
typical, 58
RAs (receiver addresses), 165
rate limiting of switches, 282
reassociation
process, 155-156
request frames, 167
response frames, 167
service, 132
receive function of PHY layer, 180
received signal strength indication (RSSI), 139
receiver addresses (RAs), 165
receivers
RF systems, role in, 42
sensitivity values of, 376

redundancy considerations, 277-282
registration testing, 409-410
reliable delivery mechanisms, 124-125
repeaters
budgeting for, 220
mechanics of, 75
range of access benefits from, 308
request-to-send/clear-to-send. *See* RTS/CTS
requirements of 802.11n, 36
requirements, defining
Acme Industries case study, 213-214
aesthetic requirements, 258-259
application requirements, 241-243, 369
approvals of, 260
budgeting phase for, 218-219
client devices, 243-244
documentation of, 259-260
elements of, list of, 241
environmental requirements, 256-258
existing infrastructure requirements, 254-255
existing systems review, 240
gathering information for, 239-240
integration requirements, 255-256
IT staff interviews, 240
mobility, 248-250
needs, distinguishing from technologies, 238
scalability, 253-254
signal coverage, 244-246
steps for, 238
tasks list for, 206-207
user interviews, 239
utilization requirements, 246-248
wireless site surveys, reviewing for, 369-370
restaurant applications, 5
restrooms, coverage issues, 245
retail WLAN markets
location-based systems for, 14
wireless advantages for, 2
retransmissions of data
ACK frames not received, 140-141
excessive, triggering dynamic rate switching, 141-142
fragmentation settings effects, 318
Retry field, MAC frames, 163
RTS/CTS effects, 318-319
Retry field, MAC frames, 163
RF amplifiers
budgeting for, 220
performance, increasing, 316
range increases from, 74-75
range of access benefits from, 307-308
role in RF systems, 42
RF bands. *See* frequency bands
RF mathematics, 53
RF shielding, 347-349
RF signal propagation. *See* propagation
RF site surveys. *See* wireless site surveys
RF spectrum, 802.11 standards comparison, 24
RF systems
amplifiers. *See* RF amplifiers
architecture of, 41
modulation, 42-45
receivers, 42
transceivers, 41-42
transmitters, 42
risk evaluation planning, 225-227
roaming
802.11 *versus* WiMAX, 27-28
access point roaming, 322-323

analyzing handoffs, 110
Announce Protocol, 323
delays from Ethernet switches, 413
disjointed cells with, 59
elements impacting, list of, 321
elevator coverage for, 333-335
handoff protocol effects, 109
Handover Protocol, 323
IAPP (Inter-Access Point Protocol), 322-323
in-motion testing, 406, 412-413
infrastructure WLAN support for, 58
ISP roaming, 324
Layer 2 roaming, 322-323, 325
Layer 3 roaming, 323-324, 325
levels and layers for, 322-324
Mobile IP, 324
mobility settings, 325-326
Proxy ARP, 324
r and k standards amendments, 323
reassociation process, 110
subnet roaming, 323-324
troubleshooting, 412-413
WiMAX roaming agreements, 29-30
wireless IP phone roaming, 324-325

robots, mobile, 6-9

rogue access points, 93-94, 346-347, 433-434

ROI (return on investment)
Acme Industries case study, 206
citywide deployments, for, 235
decisive role of, 227
timeframe for justifying deployments, 229

routers, Wi-Fi
access points compared to, 70
DHCP provided by, 70-71
functionality of, 69-70
IP address sharing with, 70-71
performance benefits of, 71
security benefits of, 72

RSSI (received signal strength indication), 139

RTS/CTS (request-to-send/clear-to-send)
access points seldom requiring, 319
b to g connections with, 22
configuring, 402
CTS frames, 173
mechanism of, 158-159
performance effects of, 318-319, 446
retransmissions of data with, 318-319
RTS frames, 173
troubleshooting, 446

S

safety
access points, distances from humans, 395
installation tips for, 389

SAs (source addresses), 165

scalability
requirements impact on site surveys, 370
requirements, defining, 253-254

scanning for networks
active scanning, 149-151
passive scanning, 149-150
probe requests, 150-151
scanning functions, 149

scheduling deployments, 217

scheduling installation activities, 390-391

scope of deployment projects, defining, 204-206

screen size issue, 291, 292
security. *See* 802.11i security
access point shut down schedules, 350
analyzing gaps in, 434
assessments, 431-434
configuration settings, reviewing, 413
denial-of-service. *See* DoS (denial-of-service) attacks
disassociation frame attacks, 95
elements of, overview, 339-340
employee policies for, 351
encryption for. *See* encryption
firmware, updating, 350
installation control policy, 425
managing, 431-434
network access privileges requirements, 251
passive monitoring vulnerability, 88-91
passwords, 443
penetration testing, 414-415
periodic testing, 426
physical inspections, 433
physical, for access points, 350
physical, location-based systems for, 14
policies, organizational, 251
policies, reviewing, 432
policies, wireless, 349-351
policy management, 425-426
pre-deployment security mechanisms, 252
printer issues, 414
public *versus* private parts of networks, 414-415
question list for analyzing requirements, 252
recommendations, 349-351
recommending improvements in, 434
requirements impact on site surveys, 369-370
requirements, defining, 250-253
RF shielding, 347-349
rogue access points, 93-94, 346-347, 433-434
sensitivity of data, determining, 250-251
SSID issues, 350
strong passwords for access points, 350
system architecture reviews, 432
testing, 406, 413-415
user interviews, 433
video surveillance vulnerability, 97
VLAN policy, 349-350
vulnerabilities overview, 87-88
WEP. *See* WEP (Wired Equivalent Privacy)
Wi-Fi routers, benefits of, 72
WPA *versus* WEP, 349
WPA. *See* WPA (Wi-Fi Protected Access)
sensitivity of receivers, 376
sensitivity, receiver, 42
sensors, unacknowledged connectionless service with, 124-125
Sequence Control field, 165
services, 802.11-defined
distribution. *See* distribution system services
station. *See* station services
session persistence, 295
shared key authentication, 151-153
shielding, RF, 347-349
short IFS, 156-157
SIFS (Short IFS), 156-157

signal coverage testers
active mode, 361
EIRPs measured by, 377-379
form factors available, 358
heat maps from, 358-359
locations, testing appropriate, 381-382
Microsoft Windows internal, 371
NetStumbler, 361-362
passive mode, 361
positioning, 360-361
simulation functions, 361
wireless site surveys, choosing for, 370-371
signal coverage testing
as-installed coverage testing, 407
beacon rate testing, 407-408
citywide system indoor coverage testing, 408
purpose of, 405
tools for, 406
tools for. *See* also signal coverage testers
wireless site survey testing, 406-407
signal coverage. *See* coverage
signal strength
amplitudes of radio waves, 41-40
attenuation of, 48-51
heat maps of, 358-361
minimum received signal strength, 376
RSSI (received signal strength indication), 139
signal coverage testers, 358-362
unit conversions for, 53
uplink *versus* downlink, 377-379
signal strength meters. *See* signal coverage testers
signal strength values, defining acceptable, 376-379
signal-to-noise ratio. *See* SNR (signal-to-noise ratio)
signals. *See* radio waves
silos, vendor, 119-120
Simple Network Management Protocol (SNMP), 425
simulation programs, 321
simulation testing, 406, 416-417
single-level facilities, channel recommendations for, 329-330
single-site VoWLAN architecture, 284-285
SIP (Session Initiation Protocol) proxies, 287
site surveys. *See* wireless site surveys
slow connections. *See* capacity; performance
SMPS (spatial multiplexing power save), 159-160
sniffing tools, 346
SNMP (Simple Network Management Protocol), 425
SNR (signal-to-noise ratio)
heat maps of, 358-361
interference effect on, 98
mechanics of, 51-54
minimum for coverage, 376
performance, effect on, 313, 316
range of access, effects on RF bands, 301
signal coverage testers, 358-362
signal power effect on range, 302-303
SOFDM (scalable orthogonal frequency division multiplexing), 27
solar power for mesh nodes, 62
source addresses (SAs), 165
spare hardware, 428
spatial multiplexing MIMO, 191-193

spatial multiplexing power save (SMPS), 159-160
spatial streams
modulation, 194-195
operation of, 191-193
spectrum analyzers
active device displays, 357
channel utilization, viewing, 375
data displayed by, 354
FFT duty cycles, 356
form factors available, 354
interference identification with, 373-375
noise floors, viewing, 374
real-time FFT displays, 354-355
recording data from, 358
swept spectrograms, 357
speed, 24. *See also* data rates
spread spectrum
direct sequence, 46. *See also* DSSS (direct-sequence spread-spectrum)
frequency hopping, 46-48
purpose of, 46
SRST (Survivable Remote Site Telephony), 286-287
SSIDs (service set identifiers)
association request frames containing, 154
configuration of, 396-397
field of frames for, 172
guest access, 345
observing, 170
penetration testing with, 414
security issues with, 350
viewing with protocol analyzers, 362-365
virtual WLANs with, 274-276, 282
SSL (Secure Sockets Layer) encryption, 90
staffing
experience level of staff, issues with, 226
identifying for deployments, 214-217
identifying for installations, 391
operational support. *See* operational support staffing
sources for potential employees, 453
training for operations and maintenance, 416
stairwells, coverage issues, 245, 336
standards. *See also* 802.11 standards
benefits of 802.11 standard, 117-120
importance of, 115
migration to future systems, 119
mixing, 120
official *versus* public standards, 115-116
price impact of, 119
proprietary wireless standards, 116
rapid development benefit, 119
station services
authentication, 130
deauthentication, 131
privacy service, 131
stations defined, 130
station states
association state, 133
authentication state, 133
frame types allowed for, 132-133
stop-and-wait ARQ, 127-128
strength of signals. *See* signal strength
strong passwords for access points, 350
subnet roaming, 323-324

subnets, scan testing, 415
Subtype field, MAC frames, 161-163
SuperScan, 414-415
supported rates field, 172
surveys, wireless. *See* wireless site surveys
Survivable Remote Site Telephony (SRST), 286-287
swept spectrograms, 357
switches, Ethernet
assessing existing for wireless site surveys, 373
autonomous access point architecture with, 265
budgeting for, 220
data rates, appropriate, 78
distribution system role, 77-79
installation of new, 393-394
rate limiting of, 282
roaming delays, unacceptable, 413
upgrading for wireless capacity, 282
synchronization, MAC layer. *See* timing and synchronization
system analysts, identifying, 215-217
system architecture design
2.4-GHz *versus* 5 GHz, 272-275
access networks. *See* access network design
ad hoc WLAN networks, 270-272
application connectivity, 264
architectural design, 264
autonomous access point architecture, 265-266
controller-based access point architecture, 267-268
distribution systems, 282-284
elements of WLAN systems, 264
mesh network architecture, 269-270
migration considerations, 276-277
recommendations, 298
redundancy considerations, 277-282
reviewing for security, 432
virtual WLANs, 274-276
VoWLAN (Voice over WLAN), 264, 284-289
system status, help desk tracking of, 423

T

TAs (transmitter addresses), 165
TCP connectivity issues, 291, 294
TCP port scanners, 414-415
teams, identifying for deployments, 214-217. *See also* staffing
technical review panels (TRPs), 430-431
telephones, WLAN. *See* VoWLAN (Voice over WLAN)
Telnet, terminal emulation with, 82
temperature requirements study, 256-257
Temporal Key Integrity Protocol (TKIP), 146
terminal emulation
advantages of, 290-291
application interfaces, enabling, 290
client/server support lacking, 291
connectivity issues, 291
disadvantages of, 291
programming environment limitations, 291
screen size issue, 291
TCP connectivity issues, 291
types of systems used with, 82-83
testing
acceptance/verification, 406, 415-416
application connectivity, 410

applications, 410-411
association performance testing, 408-409
authentication mechanisms, 410
beacon rate testing, 407-408
connectivity, 409-410
documentation, 416, 419
in-motion testing, 406, 412-413
load testing, 411
penetration testing, 414-415
performance, 406
periodic, 426
pilot testing, 406, 418
port scanners, 414-415
prototype testing, 406, 417-418
recommendations from, 419
registration testing, 409-410
reports on, 419
security, 406, 413-415
signal coverage testing, 405-408
simulation testing, 406, 416-417
support staff responsiveness, 416
types of tests to perform, 402, 405-406

TGn (High Throughput Task Group), 36

TGn Sync, 36

throughput
data rates *versus*, 141, 312-313
idle time effects on, 312-313

timestamps
frame types using, 172
in beacons, 168
peer-to-peer synchronization with, 57

timing and synchronization, MAC layer
DCF IFS, 157
Extended IFS, 157-158
PCF IFS, 157
role in MAC layer, 136
short IFS, 156-157
TSF (timing synchronization) function timers, 168

TIMs (Traffic Indication Maps), 171

TKIP (Temporal Key Integrity Protocol), 146

TNCs (terminal node controllers), 34

To DS field, MAC frames, 161

tools
access points, test, 370
antennas, test, 370
budgeting for, 221
deployment dependence of need for, 353-354
installation tools, 390
load testing, 411
port scanners, 414-415
signal testers. *See* signal coverage testers
spectrum analysis. *See* spectrum analyzers
types, list of, 354
wireless protocol analyzers, 362-365
wireless site survey tools requirements, 370-371
WireShark. *See* WireShark

training requirements for operational support staffing, 451-452

transceivers, 41-42, 64

transmission channels. *See* channels, RF

transmit beamforming, 190-191

transmit function of PHY layer, 179

transmit power configuration, 398-399

transmitter addresses (TAs), 165

transmitters, 42. *See also* client radios

trees, 51
trouble ticket systems, 435-436
troubleshooting
access point configuration issues, 445-446
access point failures, 442
ad hoc clients with access points, 443
client radios, 443-445
connections, 440-443
data rates, 445
desktop support groups, 436
firmware, 442, 445
fragmentation issues, 446
incompatibility issues, 442
interference, 442-444
methodology for, 439-440
network support groups, 436
passwords, 443
performance problems, 444-447
RTS/CTS, 446
transmit power issues, 443-445
utilization issues, 447
TRPs (technical review panels), 430-431
TSF (timing synchronization) function timers, 168
Type field, MAC frames, 161
types of WLANs
ad hoc architecture, 55-57
evolution of, 20-21
infrastructure architecture, 57-59
mesh architecture, 59-62

U

unacknowledged connectionless service, 124-125
unauthorized access
authentication systems, prevention with, 94
dangers of, 91
man-in-the-middle attacks, 92
rogue access points, 93-94
UNIX, terminal emulation for, 82-83
upgrades, evaluating, 430
uplink signal values required for coverage, 377-379
USB radio devices, 67-68
USB, Certified Wireless, 33-34
USC University Hospital VoWLAN case study, 11
users
representatives, identifying, 215-217
security interviews of, 433
utility rooms, coverage issues, 245
utilization issues
random back offs, 139
requirements, 246-248
requirements impact on site surveys, 369
troubleshooting, 447

V

verification testing, 211
VG200 voice gateways, Cisco, 11
video over WLAN
DoS attacks on, 97
retail application for, 2
WLAN application to, 10-12
VLANs (virtual LANs)
security with, 94, 349-350
system architecture design with, 274-276, 282
voice applications, 5

VoWLAN (Voice over WLAN)
ACME Industries case study, 289
adaptive channel mode issues, 332-333
advantages of, 5-10
application markets for, 5-11
architectural design considerations, 264
association performance testing, 408-409
benefits of, determining, 19, 231
call-processing agents, 287-288
CallManager, Cisco, 284-287
Cisco 7920 roaming, 325
Cisco 7920 wireless IP phone architectures, 284
edge overlap recommendations, 338
G.711 codecs, 284
gatekeepers, H.323, 287
in-motion testing of, 412-413
ISDN backups, 287
load testing, 411
mesh latency issue, 61
MGCP (Media Gateway Control Protocol) for PSTN, 285
multisite WAN with centralized processing architecture, 285-287
multisite WAN with distributed call processing, 287-288
r and k standards amendments, 323
rate limiting of switches, 282
roaming delay issues, 58
roaming solutions, 324-325
single-site architecture for, 284-285
SIP (Session Initiation Protocol) proxies, 287
SRST (Survivable Remote Site Telephony), 286-287
system architecture design, 284-289
testing, 410-411
two access point guideline, 412
USC University Hospital case study, 11
utilization requirements, 246
VG200 voice gateways, Cisco, 11
warehouses, capacity needed for, 3
VPNs (virtual private networks)
encryption with, 341
wireless issues, 349
VT (Virtual Terminal), 82-83

W

WAN capability, existing, 373
warehousing, WLANs for, 3-4
warranties, budgeting for, 221
watts, 40, 53
waves. *See* radio waves
WBSs (work breakdown structures), 206-214
weather, 51
WECA (Wireless Ethernet Compatibility Alliance), 24
WEP (Wired Equivalent Privacy)
authentication testing, 410
encryption process, 145-146
public keys for, 342
roll in failure of early 802.11 adoption, 35
shared key authentication, 151, 152-153
weakness of, 88
WEP2, 145-146
WPA recommended over, 349
Wi-Fi Alliance
certification by, 24-25
goals of, 25
protocol definition by, 18

Wi-Fi Certified logos, 25
Wi-Fi, relationship to 802.11 standards, 24
WiBro, 28
WiMAX (802.16)
3G standards with, 29
4G with, 28-29
802.16m development28
advantages over Wi-Fi, 27-28
certified equipment list for, 28
client devices for, 29
general attributes of, 26-27
IEEE standards for, 27
mobile WiMAX, 27-30
roaming agreements for, 29-30
Sprint deployment of, 29-30
TV deployment over, 28
Wi-Fi, as competition to, 30
WiMAX Forum, 18
WiMedia Alliance, 33-34
wipe functions, device, 63
wireless access networks. *See* access network design
wireless IP phone roaming, 324-325
wireless LAN. *See* WLANs (wireless LANs)
wireless middleware
Acme Industries case study, 297
advantages of, 294-296
application development tools, 296
architectural role of, 84-85
compression capabilities, 295
data bundling, 296
disadvantages of, 296
features sets, matching to applications, 297
intelligent restart capability, 295
wireless protocol analyzers, 362-365
wireless site surveys
access points, test, 370, 371
aesthetics requirements, 370
antennas, test, 370
applications requirements review, 369-370
as part of deployment design phase, 208
assessing existing infrastructure, 372-373
cell overlap considerations, 383
channel utilization, viewing, 375
citywide, 235
citywide mounting assets, evaluation of, 385-386
client device requirements, 369
communications rooms, 372
downlink signal values, 377-379
environment (facility) requirements, 370
facility inspections, 372
floor plan diagrams for, 371
identification of locations for access points, 384
interference, identifying sources of, 373-375
minimum received signal strength, 376
mobility requirements, 369
necessity of, 112-113
noise floors, viewing, 374
PoE capability, existing, 373
propagation testing, 379-383
report generation for, 385
requirements review, 369-370
scalability requirements, 370
security requirements, 369-370
signal coverage requirements, 369

signal testers, 358-362. *See also* signal coverage testers
SNR minimums, 376
spectrum analyzers for, 354-358. *See also* spectrum analyzers
steps for conducting, 368-369
switching capability, existing, 373
tools required for, 370-371
uplink signal values, 377-379
utilization requirements, 369
VoWLAN signal assurance with, 11
WAN capability, existing, 373
WireShark
active scanning test with, 151
analyzing frames with, 364-365
hacking wireless networks with, 88-91
observing typical frames, 175
WLAN markets
enterprises, general systems, 13
healthcare, 4-9
home and small office applications, 12
hospitality industry, 5
location-aware service applications, 13-15
restaurants, 5
retail, 2
video surveillance, 10-12
warehousing, 3-4
WLANs (Wireless LANs)
ad hoc architecture of, 55-57
benefits for businesses from, 2
differences with wired LANs, 130
history of, 34-37
markets for. *See* WLAN markets
WNG SC (Wireless Next Generation Standing Committee), 36
work breakdown structures (WBSs), 206-214
WPA (Wi-Fi Protected Access)
interoperability issues, 112
recommended over WEP, 349
strength of, 88
TKIP basis of, 146

X–Z

yagi antennas, 73-74
Yellowjacket signal coverage tester, 304

ZigBee, 32-33